ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ZERO-DIMENSIONAL BRANCHES OF RANK ONE ON ALGEBRAIC VARIETIES

BY SAUNDERS MACLANE AND O. F. G. SCHILLING[1]

(Received January 10, 1939)

In his fundamental investigations on the resolution of singularities of algebraic surfaces[2] O. Zariski discusses the various types of valuations on algebraic function fields of two variables. Of particular interest are branches of algebraic surfaces which can be described by zero-dimensional valuations of rank one. An interesting preliminary to the uniformization of these branches is the enumeration of the possible value groups which may occur for the corresponding valuations. We here provide a survey of all possible value groups for such valuations on $n$-dimensional algebraic varieties.

From the viewpoint of geometry it is not surprising that our results indicate that the branches can be essentially more complicated for $n$ dimensions than they are for 2-dimensional varieties. In the latter case Zariski showed that the value group $\Gamma$ of a branch is either a subgroup of the additive group of all rational numbers or can be represented as the direct sum of two infinite cyclic groups. In any event this value group must be completely reducible, in the sense that it can be represented as the sum of groups of (rational) rank[3] 1. For varieties of dimension 3 or more, we find possible value groups which are not completely reducible in this sense.

## 1. Definitions and Description of Results

DEFINITION: If $L \supset K$ are fields, we consider valuations $V$ for $L/K$, that is valuations of $L$ which prescribe the value zero for every element of $K$. Such a valuation $V$ is *zero-dimensional* if its residue class field is an algebraic extension of $K$; it has *rank* 1 if its value group $\Gamma(V)$ is a subgroup of the additive group P of all real numbers.

Let $\Gamma^{(0)}$ denote the additive group of all rational integers. A set $\tau_1, \cdots, \tau_n$ of real numbers is *rationally independent* in P if $m_1\tau_1 + \cdots + m_n\tau_n = 0$ for

[1] Johnston Scholar at the Johns Hopkins University for the year 1938–1939.

[2] O. Zariski, Reduction of singularities of an algebraic surface, these Annals, vol. 40 (1939), pp. 639–689.

[3] A group is of (rational) rank 1 if any two elements $\lambda$ and $\mu$ of the group are connected by a relation $m\lambda + n\mu = 0$, with integral coefficients $m$ and $n$. Cf. R. Baer, *Abelian groups without elements of finite order*. Duke Mathematical Journal vol. 3 (1937), pp. 68–122. This rational rank is to be carefully distinguished from the non-archimedian (ordered) rank of an ordered group. An ordered group $\Gamma$ is said to be of rank 1 in this second sense if every two positive elements $\lambda$ and $\mu$ are comparable ($m\lambda > \mu$ for some integer $m$).

$m_i$ integers only if all $m_i$ vanish. The *rank of a subgroup* $\Gamma \subset P$ is the maximal number of rationally independent elements of $\Gamma$.

A real number $\mu \in P$ is *commensurable with a subgroup* $\Gamma \subset P$ if $m\mu \in \Gamma$ for some integer $m$. A group $\Gamma' \subset P$ is *commensurable with* $\Gamma$ if every element of $\Gamma'$ is commensurable with $\Gamma$.

Our specific description of all possible value groups is as follows.

THEOREM 1. *If $L$ is an algebraic function field of $n$ variables over a field of constants $K$, and if $V$ is a rank 1 zero-dimensional valuation of $L/K$, then the value group $\Gamma(V)$ either has rank $r < n$ or has rank $n$ and is the direct sum of $n$ cyclic groups*

$$\Gamma(V) = \Gamma^{(0)}\tau_1 + \cdots + \Gamma^{(0)}\tau_n , \tag{1}$$

*in which $\tau_1 , \cdots , \tau_n$ are rationally independent real numbers.*

*Conversely, if $K$ is any field and if $\Gamma$ is a group of real numbers which has rank $r < n$ or which is the direct sum (1) of $n$ cyclic groups, the rational function field $L = K(x_1 , \cdots , x_n)$ of $n$ variables over $K$ has a rank 1 zero-dimensional valuation $V$ for $L/K$ with the given value group $\Gamma$.*

The proof of the first half of this Theorem is accomplished easily in §2. The converse part of the Theorem requires an explicit construction of a valuation V. We offer two constructions, each presented independently of the other. On the one hand, the Puiseux expansions familiar to the algebraic geometer can be so generalized as to exhibit the desired valuations if the coefficient field $K$ has characteristic 0 (§7). On the other hand, a rational construction of valuations can be carried out by algebraic analysis of the polynomial ring $K[x_1 , \cdots , x_n]$ (§§4, 5, 6).

A necessary preliminary for either method is the existence of sufficiently many algebraically independent power series over the given field $K$. This existence we establish both by an explicit construction and by a cardinal number argument in §3.

That the value groups possible according to our main theorem need not all be completely reducible follows from a known example of a group of rank 2 not so reducible, due to Pontrjagin.[4] Such examples of groups have also been investigated by Kurosch and by Baer.[5]

## 2. Analysis of the problem

To prove the first half of our main Theorem, suppose that $\Gamma(V)$ has rank $r > n$, and so contains $n + 1$ rationally independent elements $\tau_0 , \tau_1 , \cdots , \tau_n$. Pick in $L$ elements $x_i$ with $V(x_i) = \tau_i$ for $i = 0, 1, \cdots , n$. Since $L/K$ is an algebraic function field of $n$ variables, the $n + 1$ quantities $x_0 , \cdots , x_n$ of $L$

[4] L. Pontrjagin, *The theory of topological commutative groups*. Annals of Math. vol. 35 (1934), pp. 361–388; Appendix 1, example 2.

[5] A. Kurosch, *Primitive torsionsfreie abelsche Gruppen von endlichen Range*. Annals of Math. vol. 38 (1937), pp. 175–203.
R. Baer, loc. cit.

must be algebraically dependent over $K$ in accord with some polynomial relation $f(x_0, x_1, \cdots, x_n) = 0$. Since $f = 0$, at least two terms in $f$ must have the same minimum value, as required by the valuation postulates. However, the independence of the values $\tau_i$ means that no two distinct power products $x_0^{e_0} \cdots x_n^{e_n}$ can have the same value. This contradiction proves $r \leqq n$.

Secondly, suppose that $\Gamma(V)$ has rank $n$, that $\omega_1, \cdots, \omega_n$ are $n$ rationally independent elements of $\Gamma(V)$ and that $x_1, \cdots, x_n$ are elements of $L$ with $V(x_i) = \omega_i$, $i = 1, \cdots, n$. As in the last case, $x_1, \cdots, x_n$ are algebraically independent over $K$. Therefore $L$ is a finite algebraic extension of the rational function field $L_0 = K(x_1, \cdots, x_n)$. Any polynomial $f(x_1, \cdots, x_n)$ in the ring $K[x_1, \cdots, x_n]$ has exactly one term $x_1^{e_1} \cdots x_n^{e_n}$ of minimum value, $e_1\omega_1 + \cdots + e_n\omega_n$. The valuation postulates prescribe that this value is the value of $f$. Hence, in $L_0$, $V$ has the value group

$$\Gamma^* = \Gamma^{(0)}\omega_1 + \cdots + \Gamma^{(0)}\omega_n. \tag{2}$$

Since $L/L_0$ is finite algebraic, there is an integer $t$ such that every element $y$ of $L$ satisfies over $L_0$ a polynomial equation of degree $t$ or less:[6]

$$a_0 + a_1 y + \cdots + a_u y^u = 0, \qquad u \leqq t.$$

To this equation we apply a Newton Polygon argument. At least two terms $a_i y^i$ and $a_j y^j$ must have the same minimum value, hence

$$V(y) = (V(a_j) - V(a_i))/(i - j). \tag{3}$$

Therefore, using (2), the value $V(y)$ is contained in the group $(1/t!)\cdot\Gamma^*$ and $\Gamma(V)$ is a subgroup of this latter group. As subgroup of finite index in an abelian group with a basis of elements $\omega_i/t!$, $\Gamma(V)$ must itself have a basis $\tau_1, \cdots, \tau_n$, as asserted in (1) of the Theorem.

### 3. Transcendence Lemma

For the explicit construction of valuations we need

LEMMA 1. *If $K\{t\}$ is the field of all formal power series*

$$y = a_k t^k + a_{k+1} t^{k+1} + \cdots, \qquad k > -\infty$$

*with coefficients in $K$, then for each $n$ there exist $n$ such power series $y_1, \cdots, y_n$ which are algebraically independent over $K(t)$.*

FIRST PROOF (using cardinal numbers). Let $K_0$ be a finite or denumerable subfield of $K$ (e.g., the prime subfield of $K$). Then the power series field $K_0\{t\}$ is not denumerable, while the algebraic closure of the rational function field $K_0(t)$ is denumerable, so $K_0\{t\}$ certainly contains series $y_1, \cdots, y_n$ algebraically independent over $K_0(t)$. It remains only to show that they remain independent over $K(t)$.

---

[6] For instance, one can take as $t$ the reduced degree of $L/L_0$ in the sense of Steinitz, *Algebraische Theorie der Körper*, ed. by R. Baer and H. Hasse, §14.

Were $t, y_1, \cdots, y_n$ not algebraically independent over $K$, they would satisfy an algebraic relation with coefficients in a subfield $K_1$ obtained by adjoining to $K_0$ a finite number of elements. Since the adjunction of an algebraic element to $K_0$ could not make algebraically independent elements dependent, it suffices to show that $t, y_1, \cdots, y_n$ independent over a $K_1 \subset K$ remain independent over a simple transcendental extension $K_1(x) \subset K$.

A relation between $t, y_1, \cdots, y_n$ over $K_1(x)$ has the form

$$f(x, t, y_1, \cdots, y_n) = 0,$$

where $f$ is irreducible, has coefficients in $K$ and is not identically zero. But $f$ may be expressed as a power series in $t$, in which form the coefficient of each power of $t$ must be zero; that is, identically zero in $x$. Therefore we may set $x = 0$ throughout in $f$. This gives a relation $f(0, t, y_1, \cdots, y_n) = 0$ over $K_1$, contrary to assumption.

Second Proof. For a constructive theory it is more desirable to have an explicit construction of power series $y_1, \cdots, y_n$ which will be algebraically independent over $t$. F. K. Schmidt has shown that one such series $y_1$ can always be found by leaving sufficiently large gaps[7] in the series for $y_1$. It is reasonable to expect that the insertion of markedly larger gaps in the series for $y_2$ will make that quantity transcendental over $t$ and $y_1$, and so on. We now give one specific form for this gap construction.

For notation, drop all zero coefficients from a series $y$ of value zero, so that it takes the form

$$y = a_0 + a_1 t^{e_1} + \cdots + a_k t^{e_k} + \cdots; \qquad 0 < e_1 < e_2 \cdots; \qquad a_k \neq 0.$$

Denote the exponent $e_k$ of the $k + 1^{st}$ remaining term by $E_y(k)$. Construct $n$ such series $y_1, \cdots, y_n$ with any coefficients different from 0 and with rapidly increasing gaps of such sort that the corresponding functions $E_{y_i}(k) = E_i(k)$ satisfy for every $k$ the conditions

$$E_1(k+1) \geqq (k+1)E_1(k), \qquad E_1(1) \geqq 2, \tag{1}$$

$$E_i(k+1) \geqq E_{i-1}[k + 1 + kE_i(k)], \qquad E_i(1) \geqq 1, \tag{2}$$

where the second equation holds for $i = 2, \cdots, n$. Solutions for these inequalities certainly exist; for instance, we may replace them all by equalities and regard them as inductive definitions. The resulting series $t, y_1, \cdots, y_n$ are algebraically independent because any polynomial in them differs from zero and in fact has a value with a finite bound dependent only on its degree, as stated in the following lemma.

Lemma 2. *If a polynomial $f(t, y_1, \cdots, y_i)$ has degree not greater than $k$ in each variable, then*

$$V[f(t, y_1, \cdots, y_i)] < E_i(k+1), \tag{3}$$

*where $V$ is the natural series valuation of the power series field $K\{t\}$.*

[7] F. K. Schmidt, *Mehrfach perfekte Körper*, Mathemat. Annalen, vol. 108 (1933), cf. §5.

PROOF: We shall prove the lemma by induction on $i$. If $i = 1$, $y_1$ contains a gap from $E_1(k)$ to $E_1(k+1)$, so we can denote by $u$ the part of $y_1$ up to the power $E_1(k)$, where

$$y_1 = u + w, \qquad V(w) = E_1(k+1), \tag{4}$$

while $u$ has degree $E_1(k)$. The Taylor expansion of $f(t, u+w)$ is

$$f(t, u+w) = f(t, u) + wB_1(t) + w^2B_2(t) + \cdots. \tag{5}$$

Here $B_1(t)$, $B_2(t)$, $\cdots$ are polynomials in $t$, so that by (4)

$$V[wB_1(t) + w^2B_2(t) + \cdots] \geqq E_1(k+1). \tag{6}$$

If $D_t$ denotes "degree in $t$" and if

$$f(t, u) = f_0(t) + f_1(t)u + \cdots + f_m(t)u^m,$$

then any term $f_iu^i$ with $i < m$ has

$$D_t(f_iu^i) \leqq k + iE_1(k) < E_1(k) + iE_1(k) \leqq mE_1(k)$$

while the last term $f_mu^m$ has degree at least $mE_1(k)$. Therefore $f(t, u) \neq 0$ and has the value

$$V(f(t, u)) \leqq D_t(f(t, u)) \leqq D_t(f_mu^m) \leqq k + kE_1(k) < (k+1)E_1(k),$$

since $E_1(k)$ always exceeds $k$. By construction, this value does not exceed $E_1(k+1)$, hence by (5) and (6) we have the conclusion (3) of the Lemma for $i = 1$.

For the general case we again write

$$y_i = u + w, \qquad V(w) = E_i(k+1), \qquad D_t(u) = E_i(k).$$

The Taylor expansion of $f$ gives terms in $w$ with value at least $E_i(k+1)$ and a term $f(t, y_1, \cdots, y_{i-1}, u)$, so it will suffice to prove that

$$V[f(t, y_1, \cdots, y_{i-1}, u)] < E_i(k+1). \tag{7}$$

Here $u$ is a polynomial in $t$, so the whole has degree at most $k' = kE_i(k) + k$ in $t$. Apply the previous case $i - 1$ of (3) with this value of $k'$ to find

$$V[f(t, y_1, \cdots, y_{i-1}, u)] < E_{i-1}[k + kE_i(k) + 1].$$

By the construction (2), this gives the desired result (7). This completely establishes both Lemmas.

## 4. Elementary rational constructions

Our first construction of a valuation for $K(x_1, \cdots, x_n)/K$ with an arbitrarily specified value group $\Gamma$ of one of the possible types will be accomplished in three special stages: First, the construction for a value group of rank $n$; second, the addition of new variables $x_{n+1}, \cdots$, keeping the same value group; third, the addition of commensurable values to the value group (see §1, Definitions).

CONSTRUCTION I. Pick any rationally independent real numbers $\tau_1, \cdots, \tau_n$ as proposed values for $x_1, \cdots, x_n$, respectively. For any power product $y = x_1^{e_1} \cdots x_n^{e_n}$ define

$$V(x_1^{e_1} \cdots x_n^{e_n}) = e_1\tau_1 + \cdots + e_n\tau_n . \tag{1}$$

For a polynomial $f(x_1, \cdots, x_n)$ which is a sum of distinct power products $y_1, \cdots, y_s$, define

$$V(a_1y_1 + \cdots + a_sy_s) = \text{Min}\,[V(y_1), \cdots, V(y_s)]. \tag{2}$$

For a rational function set

$$V[g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n)] = V[g(x_1, \cdots, x_n)] - V[h(x_1, \cdots, x_n)]. \tag{3}$$

The resulting function $V[g/h]$ is readily seen to satisfy the valuation postulates. Its value group is $\Gamma^{(0)}\tau_1 + \cdots + \Gamma^{(0)}\tau_n$, the group of all integral combinations of $\tau_1, \cdots, \tau_n$. We shall denote this valuation of $K(x_1, \cdots, x_n)$ by

$$[Vx_1 = \tau_1, \cdots, Vx_n = \tau_n].$$

This valuation has $K$ as residue class field, hence is zero-dimensional. For the $\tau_i$ are rationally independent, hence no two distinct power products $y$ can have the same value. In any polynomial $f$ there is then exactly one term $\bar{a}\bar{y}$ of minimum value. Any residue class is given by a rational function $g/h$ of value zero. But $V(g/h) = 0$ means that $g$ and $h$ both must contain the same power product of minimum value. Hence

$$g/h \equiv \bar{a}\bar{y}/\bar{b}\bar{y} \equiv \bar{a}\bar{b} \pmod{V}.$$

This states that the residue class of $g/h$ is $\bar{a}/\bar{b}$, in $K$.

CONSTRUCTION II. We need the extension:

THEOREM 2. *If a field $L_0$ has a discrete rank one valuation $V$ such that the topological closure $\bar{L}_0$ of $L_0$ has transcendence degree at least $m$ over $L_0$, then the valuation $V$ can be extended to a field $L_0(x_1, \cdots, x_m)$ of rational functions of $m$ independent variables in such a way that its value group and residue-class field remain unchanged.*

PROOF. For an existence proof, one need only pick out of $\bar{L}_0$ $m$ quantities $y_1, \cdots, y_m$ algebraically independent over $L_0$. The field $L_0(y_1, \cdots, y_m) \subset \bar{L}_0$ then has a valuation of the required sort and is equivalent to the given field $L_0(x_1, \cdots, x_m)$.

Another form of this argument gives a rational computation for the values of polynomials in the $x_i$. Since we can add one variable $x$ at a time, and since the field $L_0' = L_0(x_1, \cdots, x_k)$ obtained at any stage has a complete field of transcendence degree at least $m - k$ over $L_0'$, it suffices to consider the case when $m = 1$. Let $\{a_k\}$ be a convergent sequence of elements in $L_0$, whose limit $\alpha$ in $\bar{L}_0$ is transcendental over $L_0$. For any polynomial $f(x)$ in $L_0(x)$ define

$$W[f(x)] = \lim_{k\to\infty} V[f(a_k)]. \tag{4}$$

If $f$ is not identically 0, this limit is not $\infty$ because $\alpha$ is transcendental over $L_0$ and so does not satisfy the equation $f(\alpha) = 0$. The sum and product laws are readily verified for $W$. Hence $W$, extended to rational functions as in (3), is a valuation of $L_0(x)$ with the required value group. One can show that its residue class field is the same as that of $L_0$.

## 5. The infinite rational construction

Let a field $K$ have a rank 1 valuation $V$ with a value group $\Delta$ and let $L = K(x)$ be a field of rational functions over $K$, while $\Gamma \supset \Delta$ is a denumerable group of real numbers commensurable with $\Delta$ such that $\Gamma/\Delta$ is infinite. We propose to construct[8] a valuation of $K(x)$ with value group $\Gamma$.

Since $\Gamma$ is denumerable, $\Gamma$ can be obtained from $\Delta$ by the group-adjunction of a denumerable set of positive elements $\mu_1, \mu_2, \cdots$. Let $\Gamma_m$ be the group obtained by adjoining the first $m$ generators $\mu_i$, so that $\Gamma_m$ consist of all real numbers

$$\delta_0 + s_1\mu_1 + \cdots + s_m\mu_m \qquad (\delta_0 \in \Delta,\ s_i \text{ integers}). \tag{1}$$

Let $t_m$ denote the index of $\Gamma_{m-1}$ in $\Gamma_m$. Since $\Gamma/\Delta$ is infinite, we can suppose that none of the generators $\mu_m$ is unnecessary; hence each $t_m > 1$. Each generator $\mu_m$ can be increased by any positive element from $\Gamma_{m-1}$, hence we can assume

$$\mu_{m+1} > t_m\mu_m, \qquad t_m > 1, \qquad (m = 1, 2, \cdots). \tag{2}$$

Each $t_m$ is the smallest integer such that $t_m\mu_m$ is in $\Gamma_{m-1}$ (where $\Gamma_0$ means $\Delta$). By (1),

$$t_m\mu_m = \delta_m + s_{m1}\mu_1 + s_{m2}\mu_2 + \cdots + s_{m,m-1}\mu_{m-1}, \qquad (m = 1, 2, \cdots), \tag{3}$$

where each $\delta_m \in \Delta$ and each $s_{mi}$ is so reduced that $0 \leqq s_{mi} < t_i$.

For our purposes it will suffice to construct a valuation of $K(x)$ in which each group generator $\mu_m$ is the value of some polynomial $\phi_m = \phi_m(x)$. As $\phi_1(x)$ we choose $x$ itself, and then define the general polynomial $\phi$ by induction as

$$\phi_{m+1}(x) = \phi_m^{t_m} - U_m \qquad (m = 1, 2, \cdots), \tag{4}$$

where $U_m$ is a polynomial constructed from the coefficients of (3). Thus

$$U_m(x) = a_m\phi_1^{s_{m1}}\phi_2^{s_{m2}} \cdots \phi_{m-1}^{s_{m,m-1}} \qquad (m = 1, 2, \cdots), \tag{5}$$

and where $a_m$ is any element in $K$ with $V(a_m) = \delta_m$. In this definition (4) the term $U_m$ has smaller degree than $\phi_m^{t_m}$. Specifically, if $d_m = t_1t_2 \cdots t_{m-1}$, an induction from the hypothesis $t_m \geqq 2$ of (2) proves that $d_1 + d_2 + \cdots + d_m < d_{m+1}$. Another induction then proves that

$$\text{degree } (\phi_{m+1}) = d_{m+1} = t_1t_2 \cdots t_m = t_m[\text{degree } \phi_m], \tag{6}$$

[8] The construction given is essentially a special case of one used to find all discrete valuations of a polynomial ring. See Saunders MacLane, *A construction for absolute values in polynomial rings*, Trans. of the Am. Math. Soc., vol. 40 (1936), pp. 363–395.

for in the definition (4) the first term $\phi_m^{t_m}$ has degree $t_m d_m = d_{m+1}$, while the second term $U_m$ has a degree smaller than $d_2 + d_3 + \cdots + d_m < d_{m+1}$.

THEOREM 3. *If $V$ is a valuation of a field $K$ with a value group $\Delta$, if $\Gamma \supset \Delta$ is a denumerable group of real number commensurable with $\Delta$ such that $\Gamma/\Delta$ is infinite, if $\Gamma$ is generated from $\Delta$ by the numbers $\mu_m$ of (2), and if $L = K(x)$ is a field of rational functions over $K$, then the valuation $V$ of $K$ has exactly one extension to a valuation $W$ of $L_1$ in which each polynomial $\phi_m$ of (4) has value $\mu_m$. This extended value $W$ has value-group $\Gamma$ and a residue-class field identical with the residue-class field of $V$ in $K$.*

PROOF. For the uniqueness of the extension $W$, we expand any polynomial $f(x)$ in terms of the $\phi$'s. To this end, pick $m$ so large that the degree of $\phi_{m+1}(x)$ exceeds that of $f(x)$, and divide $f(x)$ successively by $\phi_m(x)$ to obtain a first expansion

$$f(x) = f_0(x) + f_1(x)\phi_m + \cdots + f_r(x)\phi_m^r \tag{7}$$

with coefficients $f_i(x)$ each of degree less than $d_m$. The degree of $\phi_m^r$ must be less than that of $\phi_{m+1}$, so $r < t_m$. Each coefficient $f_i(x)$ may in turn be expanded in powers of $\phi_{m-1}$, so that we eventually obtain a representation of $f(x)$ as a sum of terms

$$f(x) = T_1 + \cdots + T_s \tag{8}$$

where each power product $T_j$ has the form

$$T = a\phi_1^{e_1} \cdots \phi_m^{e_m}, \qquad 0 \leqq e_i < t_i \qquad (i = 1, \cdots, m), \tag{9}$$

for $a$ in $K$. The expansion (8) for $f(x)$ in terms like (9) is unique, as one can show by induction.

The value of any single term $T$ of (9) is necessarily given by

$$W(T) = V(a) + e_1\mu_1 + \cdots + e_m\mu_m. \tag{10}$$

Because the exponents $e_i$ are limited by the indices $t_i = [\Gamma_i : \Gamma_{i-1}]$, it follows that *no two terms $T_i$, $T_j$ like (9) can have the same $W$ value.* Hence the value of the polynomial $f(x)$ of (8) is necessarily

$$W[f(x)] = \text{Min}\,[W(T_1), \cdots, W(T_s)], \tag{11}$$

while the value of a rational function $f(x)/g(x)$ is

$$W[f(x)/g(x)] = W[f(x)] - W[g(x)]. \tag{12}$$

This proves that $V$ has but one extension with $W\phi_m = \mu_m$.

Conversely, we must show that the function $W$ defined from the expansion (8) by the equations (10), (11), (12) is always a valuation of $K(x)$. The usual property for the value of the sum of two polynomials is proved readily, while

that for the value of a product[9] may be deduced once we prove the same property for the product of two terms $T_i$ and $T_j$. This product then has the form $T' = b\phi_1^{h_1} \cdots \phi_m^{h_m}$, and it suffices to show that $W(T')$ is given by the function

$$W'(b\phi_1^{h_1} \cdots \phi_m^{h_m}) = Vb + h_1\mu_1 + \cdots + h_m\mu_m . \tag{13}$$

In other words, the value of a term with unlimited exponents $h_i$ is computed exactly as in (10). To prove this we must find the expansion of $T'$ by successive substitutions of (4). If $T'$ has an exponent $h_k \geqq t_k$, then $T' = S\phi_k^{t_k}$, where $S$ is another term. By (4)

$$T' = S\phi_k^{t_k} = S\phi_{k+1} + SU_k. \tag{14}$$

By (3) and the construction (5) of $U_k$, the second term here has

$$W'(SU_k) = W'(S) + t_k\mu_k = W'(S\phi_k^{t_k}).$$

For the first term, however, the choice of $\mu_k$ in (2) proves

$$W'(S\phi_{k+1}) = W'(S) + \mu_{k+1} > W'(S) + t_k\mu_k = W'(S\phi_k^{t_k}).$$

Thus (14) expresses $T'$ as a sum of two terms, one with the same $W'$-value as $T'$, the other with a larger $W'$-value. Repeated substitutions like (14) eventually will yield the complete[10] expansion (8) for $T'$, and in this expansion exactly one term $T_i'$ will have $W'(T_i') = W'(T')$, while all the other terms $T_j'$ for $j \neq i$ have $W'(T_j') > W'(T')$. Therefore $W(T) = \text{Min}\,[W'(T_i')] = W'(T_i') = W'(T')$. Thus (13) does give $W(T)$, as required for the product law.

It remains only to obtain the value group and residue class field for this valuation $W$. That the value group is $\Gamma$ is clear because the definition expresses all $W$-values in terms of the given generators $\mu_m$ of $\Gamma$. As for the residue class field, consider any rational function $f(x)/g(x)$ of value zero. In the expansion (8) for numerator or denominator only one term $\phi_1^{e_1} \cdots \phi_m^{e_m}$ can have minimum value, and these two terms of minimum value must have the same value, hence must have the same exponents. Therefore

$$\frac{f(x)}{g(x)} \equiv \frac{a\phi_1^{e_1} \cdots \phi_m^{e_m}}{b\phi_1^{e_1} \cdots \phi_m^{e_m}} \equiv \frac{a}{b} \pmod{W}.$$

This states that the residue class of $f/g$ is the residue class of an element $a/b$ from $K$. Hence the residue class field[11] is exactly that of $K$.

---

[9] That $W$ is a value of $K(x)$ may be also shown by reference to the results of MacLane, loc. cit. In the terminology used there, $W$ is a "limit value" defined by the "key polynomials" $\phi_m$. It is necessary to show that each $\phi_m$ satisfies the definition of a "key," and this is the case because each $\phi_m$ has a linear image over a residue class field (loc. cit. Theorem 4.2, Definition 4.1, Theorem 9.4 and condition (iii a) of page 388). The special case is given in detail above because it is appreciably simpler than the general case treated in the paper referred to.

[10] To see that the process (4) ultimately comes to an end, note that it breaks $T'$ into two terms, one of smaller degree, the other of the same degree, but with a larger number of factors $\phi$ for which $j > k$. Hence it cannot be repeated indefinitely.

[11] This also follows from MacLane, loc. cit., Theorem 14.1.

## 6. The composite rational construction

The several methods given can be combined to give a construction of a zero-dimensional valuation for $K(x_1, \cdots, x_n)$ with any allowable value group $\Gamma$.

In the first case, if the given value group $\Gamma$ has rank $n$, then $\Gamma = \Gamma^{(0)}\tau_1 + \cdots + \Gamma^{(0)}\tau_n$. The valuation $[Vx_1 = \tau_1, \cdots, Vx_n = \tau_n]$ of §4 has this value group.

If $\Gamma$ has rank $r < n$, let $\Delta$ be a subgroup generated by $r$ rationally independent elements $\tau_1, \cdots, \tau_r$. If $\Delta$ has a finite index in $\Gamma$, the group $\Gamma$ itself must have a finite basis, so that we can choose the $\tau_i$ so that $\Delta = \Gamma$. Passing to an isomorphic group, we can make $\tau_1 = 1$. We first construct a valuation $V_1$ for $K(x_1)$ by setting $Vx_1 = 1$, as in §4. The complete closure of the field $K(x_1)$ is then the field of power series in $x_1$, hence the transcendence Lemma shows that $V_1$ can be extended to a valuation $V'$ of the field $K(x_1, x_2, \cdots, x_{n-r+1})$, without changing the residue-class field or the value group $\Gamma^{(0)}$. The remaining group generators may then be introduced by the method of §4, with $[Vx_{n-r+2} = \tau_2, \cdots, Vx_n = \tau_r]$.

In the final case, the subgroup $\Delta$ has an infinite index in $\Gamma$. By the methods just used, we can first obtain for the subfield $L = K(x_1, \cdots, x_{n-1})$ a zero-dimensional valuation $V_0$ with the value group $\Delta$. Then $\Gamma$ can be generated over $\Delta$ by a denumerable sequence $\mu_1, \mu_2, \cdots$, so the methods of §5 yield an extension of $V_0$ from $L$ to the field $L(x_n)$ which will realize the given value group $\Gamma$. This establishes the converse of Theorem 1.

## 7. Generalized Puiseux expansions

Let $\Gamma$ be a given group of real numbers of rank $r + 1$ and construct over a coefficient field $K$ the set of all formal series

$$y = a_0 t^{\gamma_0} + a_1 t^{\gamma_1} + a_2 t^{\gamma_2} + \cdots \tag{1}$$

with coefficients $a_i$ in $K$ and with exponents $\gamma_i$ from $\Gamma$ so chosen that $\gamma_0 < \gamma_1 < \gamma_2 < \cdots$ and $\lim \gamma_n = \infty$. The set $K\{t, \Gamma\}$ of all these series with the usual formal rules for addition and multiplication is a field. It has a rational valuation $V$ with

$$V(y) = \gamma_0 \qquad \text{if } y \text{ in (1) has } a_0 \neq 0. \tag{2}$$

In this valuation $V$, $K\{t, \Gamma\}$ is complete and has $\Gamma$ as its value group.

For the rational function field $K(x_1, \cdots, x_n)$ one can now determine a valuation $V^*$ by choosing for each variable $x_i$ a series expansion $y_i$ of the form (1), which we may call a *generalized Puiseux expansion* of $x_i$. If the $y_1, \cdots, y_n$ are algebraically independent over $K$, as in the Lemma 1 of §3, these expansions determine an isomorphic mapping of $K(x_1, \cdots, x_n)$ on the power series field $K\{t, \Gamma\}$. This map carries the given series valuation $V$ into a valuation $V^*$ of $K(x_1, \cdots, x_n)$, with a value group $\Gamma^*$ which is a subgroup of $\Gamma$. The exact nature of $\Gamma^*$ may be determined by a generalized Puiseux argument now to be given.[12]

[12] Compare the analysis in O. F. G. Schilling, A generalization of local class field theory, American Journ. of Math. vol. 60 (1938), pp. 667–704, especially §6.

If the given group $\Gamma$ of rank $r+1$ contains rationally independent numbers $1, \tau_1, \cdots, \tau_r$, we can certainly pick as $r+1$ independent power series the quantities $t, t^{\tau_1}, \cdots, t^{\tau_r}$. The rational functions of these quantities give a value group $\Gamma^{(0)} + \Gamma^{(0)}\tau_1 + \cdots + \Gamma^{(0)}\tau_r$; it remains to find the value group given by adjoining another series (1).

LEMMA 3. *If $K\{t, \Gamma\}$ is the power series field with coefficients in an algebraically closed field $K$ of characteristic 0 and with exponents in a group $\Gamma$ of real numbers with basis $1, \tau_1, \cdots, \tau_r$, while $L^*$ is a subfield of $K\{t, \Gamma\}$ containing $t, t^{\tau_1}, \cdots, t^{\tau_r}$ and having in the valuation $V$ of (2) a value group $\Gamma^*$, then the field $L^*(y)$ obtained by adjoining $y$ of (1) to $L^*$ has in $V$ the value group $\{\Gamma^*, \gamma_0, \gamma_1, \gamma_2, \cdots\}$.*

PROOF. It suffices to show by induction that each exponent $\gamma_k$ of (1) is the value of a suitable function in $L^*(y)$. For the initial $\gamma_0$, $y$ itself is such a function, hence we assume that this is proven through $\gamma_{k-1}$ and that the $k^{\text{th}}$ exponent is not an integral combination of the preceding ones and elements of $\Gamma^*$. We want to show that $\gamma_k$ is in the value group. Put

$$y = \sum_{i=0}^{k-1} a_i y^{\gamma_i} + a_k t^{\gamma_k} + \sum_{i=k+1}^{\infty} a_i t^{\gamma_i} \tag{3}$$
$$= S + a_k t^{\gamma_k} + T.$$

Let $A_k$ be the (abelian) extension of $L^*(y)$ which arises by adjoining the element $S$, and let $g$ be any automorphism of $A_k/L^*(y)$. We find that

$$P_k = \prod_{(g)} (y - S^g)$$

is an element of $L^*(y)$, for it may be considered as a polynomial in $y$ with coefficients which are in $A_k$ and which are unaltered by every $g$. It remains to compute the value of $P_k$.

An automorphism $g$ carries $S$ into

$$S^g = \left(\sum_{i=0}^{k-1} a_i t^{\gamma_i}\right)^g = \sum_{i=0}^{k-1} a_i \zeta_{ig} t^{\gamma_i}, \tag{4}$$

where the $\zeta_{ig}$ are suitable roots of unity. For, every exponent $\gamma_i$ has some multiple $m_i$ which is a linear combination of the basis $1, \tau_1, \cdots, \tau_r$ of the group $\Gamma$. Since $t$ and $t^{\gamma_i}$ are in $L^*$, this means that $(t^{\gamma_i})^{m_i}$ is in $L^*$. Therefore each $g$, extended in any fashion to the field containing all $t^{\gamma_i}$, must carry each $m_i^{\text{th}}$ root $t^{\gamma_i}$ into some $\zeta_{ig} t^{\gamma_i}$, where $\zeta_{ig}$ is a root of unity lying in the algebraically closed coefficient field $K$. This proves (4).

By the construction of $S$ in (3), the factor $y - S$ of $P_k$ has value $\gamma_k$. In each other factor $S^g \neq S$ because $A_k$ must be separable over the field $L^*(y)$ of characteristic 0. Thus at least one coefficient $a_i\zeta_{ig}$ of $S^g$ in (4) is different from the corresponding coefficient $a_i$ of $S$, and the value of $y - S^g$ is the exponent $\gamma_i$ for the first such coefficient.

Thus the value $V(P_k)$ differs from $\gamma_k$ by an integral combination $\delta_k$ of the preceding exponents,

$$V(P_k) = \gamma_k + \delta_k.$$

Since there exists according to induction an element $Q_k$ of $L^*(y)$ whose value equals $\delta_k$, we get in $P_kQ_k^{-1}$ an element of $L^*(y)$ whose value is equal to $\gamma_k$. Consequently the value group $\Gamma'$ of $L^*(y)$ contains $\{\Gamma^*, \gamma_0, \gamma_1, \cdots\}$. Since $V$ is a valuation, it immediately follows that

$$\Gamma' = \{\Gamma^*, \gamma_0, \gamma_1, \cdots\}.$$

Repeated applications of this process yield

THEOREM 4. *If $m$ power series $y_1, \cdots, y_m$ with*

$$y_j = a_{0j}t^{\gamma_{0j}} + a_{1j}t^{\gamma_{1j}} + a_{2j}t^{\gamma_{2j}} + \cdots \qquad (\lim_{i=\infty} \gamma_{ij} = \infty) \tag{5}$$

*have coefficients $a_{ij}$ all $\neq 0$ in a field $K$ of characteristic 0 and have exponents $\gamma_{ij}$ which are rational linear combinations of $r+1$ given real numbers $1, \tau_1, \cdots, \tau_r$, then the field $K(t, t^{\tau_1}, \cdots, t^{\tau_r}, y_1, \cdots, y_m)$ has in the natural series value $V$ of (2) a value group generated by $1, \tau_1, \cdots, \tau_r$ and all the exponents $\gamma_{ij}$ of the given series (3), for $j = 1, \cdots, m$.*

PROOF. The Lemma 3 gives this theorem in case $1, \tau_1, \cdots, \tau_r$ are rationally independent, and a supplementary argument readily shows the same result if they are dependent. It remains only to remove the restriction, used in the Lemma, that $K$ be algebraically closed.

Let $K(x_1, \cdots, x_n)$ be the field $K(t, t^{\tau_1}, \cdots, t^{\tau_r}, y_1, \cdots, y_m)$ of the Theorem. Consider the algebraic closure $\bar{K}$ of $K$. We know already that the series value $V$ of $\bar{K}(x_1, \cdots, x_n)$ has the required value group. We need only show that $K(x_1, \cdots, x_n)$ has the same value group. Suppose that its group $\Gamma_0$ were smaller than $\Gamma$, that $\delta$ is an element of $\Gamma$ not in $\Gamma_0$, and that $z$ is an element of $\bar{K}(x_1, \cdots, x_n)$ with value $\delta$. Write $z$ as a rational function of $x_1, \cdots, x_n$ and let $K'$ be the finite algebraic extension of $K$ generated by the coefficients of this rational function. Then $z$ lies in $K'(x_1, \cdots, x_n)$, so that this field is ramified over $K(x_1, \cdots, x_n)$. On the other hand, these fields have respectively the residue class fields $K'$ and $K$, so that $K'(x_1, \cdots, x_n)$ is an inertial extension of $K(x_1, \cdots, x_n)$ in the valuation $V$. It cannot then be ramified. This contradiction proves $\Gamma_0 = \Gamma$, and with it the Theorem.

From this Theorem we can now construct valuations of $K(x_1, \cdots, x_n)$ with any specified possible value group $\Gamma$. If $\Gamma$ has rank $n$, with a basis $1, \tau_2, \cdots, \tau_n$ the field $K(t, t^{\tau_2}, \cdots, t^{\tau_n})$ gives the required valuation. If $\Gamma$ has rank $r+1 < n$ and has a basis $1, \tau_1, \cdots, \tau_r$ we need only map $K(x_1, \cdots, x_n)$ on the field $K(t, t^{\tau_1}, \cdots, t^{\tau_r}, y_1, \cdots, y_m)$ of the Theorem, taking care to insure that the exponents $\gamma_{ij}$ in (3) generate the whole group $\Gamma$ and that the quantities $t, t^{\tau_1}, \cdots, t^{\tau_r}, y_1, \cdots, y_m$ are algebraically independent.

A specific form of this insurance is as follows: Let $\Delta$ be the group of all integral linear combinations of $1, \tau_1, \cdots, \tau_r$. If $\Delta$ has a finite index in $\Gamma$, $\Gamma$ is also a group with a basis of $r+1$ elements, so that we can so choose the $\tau_i$ that $\Delta = \Gamma$. For $y_1, \cdots, y_m$ we may then use any series in integral powers of $t$ which are algebraically independent over $K(t)$, as in Lemma 1 of §3. Over the field

$K(t, y_1, \cdots, y_m)$ the $t^{r_1}, \cdots, t^{r_r}$ are algebraically independent because of the rational independence of their exponents.

If $\Gamma/\Delta$ is infinite, $\Gamma$ may be generated from $\Delta$ by a denumerable set of real numbers $\gamma_0 < \gamma_1 < \gamma_2 < \cdots$ with $\gamma_i \to \infty$ (cf. §5). Let $y_m$ be a series (1) with these exponents and with all its coefficients $\neq 0$. As in the previous case we can pick $y_1, \cdots, y_{m-1}$ as series in integral powers of $t$ so that $t, t^{r_1}, \cdots, t^{r_r}$, $y_1, \cdots, y_{m-1}$ are algebraically independent. The last series $y_m$ must also be algebraically independent because its adjunction yields an infinite extension of the value group $\Delta$.

This construction establishes the part of our main Theorem (in §1) which asserts the existence of valuations with given $\Gamma$, at least for coefficient fields $K$ of characteristic 0.

We wish to make some final remarks on a problem which is intimately related to our results. Suppose as before that $L = K(x_1, \cdots, x_n)$ is a function field on which a rank 1 zero-dimensional valuation $V$ is given. Then $L$ can be imbedded isomorphically in the maximally complete field $K\{t, \Gamma\}^*$.[13] Without loss of generality we may suppose that $x_1, \cdots, x_n$ lie in the valuation ring $B$ of $K\{t, \Gamma\}$. Therefore

$$x_1 = t, \qquad x_i = x_i(t); \qquad\qquad i = 2, \cdots, n$$

for a suitable imbedding of $L$ in $K\{t, \Gamma\}$. The series $x_i(t) = \sum a_{ij}t^{\alpha_{ij}}$ will in general not be power series of type $\omega$.

Let us associate to the power series $x_2(t)$ a new power series $x_2' = x_2'(t)$ in $K\{t, \Gamma\}^*$ which either consists of the single term $t^\tau$ (where $\tau$ is irrational) or is given as $\sum a_j t^{\alpha_j}$ where the infinite sum $\sum a_j t^{\alpha_j}$ is the first $\omega$-sum in the general development of $x_2$ ($\alpha_j$ all rational). In this case Zariski remarks[14] that one obtains $V[f(x_1, x_2)]$, where $f(x_1, x_2)$ is an arbitrary polynomial of $x_1, x_2$, as the leading exponent of $f(x_1, x_2')$ by omitting all terms in $f(x_1, x_2')$ which appear after the first $\omega$-sequence. Let $x_2 = a_0 t^{\alpha_0} + \cdots + a_i t^{\alpha_i} + \cdots + p(t)$, where $p(t)$ is a power series of $t$ with exponents in $\Gamma$ such that

$$V[p(t)] \geqq \lim \gamma_i < \infty.$$

Namely, then we get $f(x_1, x_2) = \prod_{(i)} (x_2 - x_2^{(i)})$ where $x_2^{(i)} = x_2^{(i)}(t^{1/\nu_i})$; the $\nu_i$ are integers which are bounded by the degree of $f(x_1, x_2)$ with respect to $x_2$. Hence not all exponents $\alpha_i$ can cancel for the $x_2^{(i)}$ are $\omega$-sequences in $t^{1/\nu_i}$ and all of these series are distinct from $x_2$.

Such a substitution simplifies the study of the value group $\Gamma$ of $V$. One is able to apply the customary arguments of the theory of Puiseux expansions. It turns out that the exponents $\alpha_i$ of $x_2'$ determine a set of generators (not necessarily a minimal set) of $\Gamma$.

---

[13] Here $K\{t, \Gamma\}^*$ denotes the field of all formal power series with coefficients in $K$ and exponents in $\Gamma$. The series have any type of ordering compatible with the ordering type of $\Gamma$.

[14] Loc. cit. (2).

There arises the problem whether a similar simplification of the series $x_i(t)$ can be carried out for fields of more than 2 variables. In particular, one should like to find a method which enables one to determine the value group $\Gamma(V)$ just by inspection of a set of defining power series. Any result in this direction will surely indicate structural properties of the singularities on $n$-dimensional algebraic varieties.

HARVARD UNIVERSITY AND
THE JOHNS HOPKINS UNIVERSITY.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# A CLASS OF ORTHOGONAL FUNCTIONS ON PLANE CURVES[1]

BY DUNHAM JACKSON

(Received March 20, 1939)

## 1. Introduction

From the beginning there is a close but not complete parallelism between the theory of approximation by polynomials and that of approximation by trigonometric sums. This is true both for the orthogonal developments in Legendre and Fourier series and for approximation by more general linear combinations of the fundamental monomials. From another point of view, the Legendre and Fourier series may be regarded as special cases under a theory of polynomials orthogonal on curves in the plane of a pair of real variables, the curve being a line segment in one case and a circle in the other.[2]

The notion of orthogonal polynomials on a plane curve may again be varied by replacing the polynomials by trigonometric sums. The purpose of the following pages is to clarify some of the changes in the theory that are brought about by this replacement. A natural procedure would be to pass directly from polynomials in two variables to double trigonometric sums. It is somewhat simpler, however, to deal with expressions which are trigonometric sums in one variable and polynomials in the other. Such an expression, a trigonometric sum in $x$ with coefficients which are polynomials in $y$, or a polynomial in $y$ with coefficients which are trigonometric sums in $x$, will be called here simply a *mixed sum*. The next sections will be concerned mainly with the beginnings of a theory of orthogonal mixed sums on a curve which is itself characterized by the vanishing of a particular mixed sum, the analogue of an algebraic curve in the case of ordinary polynomials.

By another change in point of view the problem can be regarded as pertaining to polynomials in three variables on an algebraic curve in space.[3] If $u = \cos x$, $v = \sin x$, a mixed sum $S(x, y)$ is a polynomial $P(u, v, y)$, and the curve $S(x, y) = 0$ corresponds to the curve defined by the simultaneous vanishing of $P(u, v, y)$ and $u^2 + v^2 - 1$. It will be convenient however to work with the formulation in terms of two variables.

The discussion of mixed sums will be followed by a brief indication of some of the novel features which are encountered for the first time when the orthogonal functions are trigonometric with respect to both variables. The double trigo-

[1] Presented to the American Mathematical Society September 6, 1938.

[2] See D. Jackson, *Orthogonal polynomials on a plane curve*, Duke Mathematical Journal, vol. 3 (1937), pp. 228–236.

[3] See D. Jackson, *Orthogonal polynomials in three variables*, Duke Mathematical Journal, vol. 4 (1938), pp. 441–454.

nometric sums which are orthogonal on a curve can naturally be regarded as polynomials in four variables orthogonal on a one-dimensional curve in four-dimensional space, but that aspect of the theory will not be further developed here.

## 2. Constitution of systems of orthogonal mixed sums

A mixed sum is a linear combination of a finite number of the monomials.

$$(1) \qquad 1,\ \cos x,\ \sin x,\ y,\ \cos 2x,\ \sin 2x,\ y\cos x,\ y\sin x,\ y^2,\ \cdots.$$

The terms $y^q \cos px$, $y^q \sin px$ will be said to be of *rank* $(p, q)$. Of two ranks $(p, q)$, $(p', q')$, the latter will be said to be higher if $p' + q' > p + q$, or if $p' + q' = p + q$ and $q' > q$; the monomials (1) are arranged in order of non-decreasing rank. The term or pair of terms of highest rank in a mixed sum will be called its *leading term* or terms. This highest rank will be called the rank of the mixed sum; if it is $(p, q)$, the sum is of *order* $p + q$. If a sum of rank $(p, q)$ and order $n$ is multiplied by a sum of rank $(p', q')$ and order $n'$ the product is of rank $(p + p', q + q')$ and order $n + n'$. There will be occasion also to speak of the order of a mixed sum with respect to the single variable $x$; this order is not necessarily the same as either $p$ or $n$. For brevity, when no confusion is likely to result, a sum will sometimes be said to be of order $n$ when it is of order $n$ *at most*. A coefficient will be omitted on occasion in applying the designation "leading term."

The construction of a system of mixed sums orthogonal over a two-dimensional region is a mere matter of the application of Schmidt's process to the monomials (1), and offers no significant novelty from the point of view of the present discussion. The same is true for orthogonality along a curve on which no mixed sum is identically zero, i.e. a curve on which there is no relation of linear dependence connecting a finite number of the monomials.

To proceed to the case which is of immediate interest, let $C$ be a curve on which a mixed sum $\Omega_0(x, y)$ vanishes identically. For simplicity let $C$ be of finite length, and contained in the strip $-\pi < x < \pi$. Even in this period strip it is not assumed necessarily to constitute the entire locus of the equation $\Omega_0(x, y) = 0$. The leading term, or one of the leading terms, of $\Omega_0$ or of any mixed sum divisible by $\Omega_0$ is linearly expressible on $C$ in terms of monomials preceding it in the sequence (1). It is to be inquired what monomials from (1) retain their linear independence, to serve as basis for the construction of an orthogonal system. Integration is to be performed with respect to arc length, and the integrals are to be thought of as involving a weight function $\rho(s)$ which is non-negative, integrable, and positive on a set of positive measure.

The transformation

$$z = \tan\frac{x}{2}, \qquad \cos x = \frac{1 - z^2}{1 + z^2}, \qquad \sin x = \frac{2z}{1 + z^2}$$

associates with $C$ a finite curve $C'$ in the $(z, y)$ plane. *Any mixed sum $S(x, y)$ which is of order $r$ as a trigonometric sum in $x$ has the form $P(z, y)/(1 + z^2)^r$, where $P(z, y)$ is a polynomial of degree $2r$ at most in $z$; and any such fraction in which the degree of the numerator with respect to $z$ does not exceed $2r$ is expressible as a mixed sum in $x$ and $y$.* In particular, if $\Omega_0$ is of order $r_0$ in $x$, $\Omega_0$ has the form $\omega_0(z, y)/(1 + z^2)^{r_0}$. The polynomial $\omega_0(z, y)$ vanishes identically on $C'$. Among all polynomials vanishing identically on $C'$ there is one and essentially just one which is of lowest degree in the two variables together. Let this polynomial, with some determination of the constant factor, be denoted by $\omega(z, y)$. Let its degree with respect to $z$, even or odd according to circumstances, be $2r$ or $2r - 1$. Every polynomial which vanishes identically on $C'$ is divisible by $\omega(z, y)$. The expression

$$\Omega(x, y) = \frac{\omega(z, y)}{(1 + z^2)^r}$$

is a mixed sum in $x$ and $y$ vanishing identically on $C$.

Let $\Omega_1(x, y) = \omega_1(z, y)/(1 + z^2)^{r_1}$ be any other mixed sum vanishing on $C$, of order $r_1$ with respect to $x$. *Suppose first that the degree of $\omega$ in $z$ is $2r$.* In the factorization $\omega_1(z, y) = \psi(z, y)\omega(z, y)$, the polynomial $\psi(z, y)$ is of degree $2(r_1 - r)$ (at most) in $z$. The function

$$\Psi(x, y) = \frac{\psi(z, y)}{(1 + z^2)^{r_1 - r}} \tag{2}$$

is a mixed sum in $x$ and $y$, and $\Omega_1(x, y) = \Psi(x, y)\Omega(x, y)$. *The sum $\Omega_1$ is divisible by $\Omega$.*

Let the leading terms of $\Omega$ be $Ay^q \cos px + By^q \sin px$, $A^2 + pB^2 \neq 0$, $p + q = N$. If $\Omega_1$ is of order $n$ its rank $(h, k)$ must satisfy the conditions

$$h \geqq p, \qquad k \geqq q, \qquad h + k = n, \qquad h = n - k \leqq n - q = p + n - N.$$

So $h$ must have one of the values $p, p + 1, \cdots, p + n - N$. Furthermore, if $h = p$ then the leading term of $\Psi$ can not involve $x$, and for $p > 0$ the term $y^{n-p} \sin px$ is necessarily present or necessarily absent in $\Omega_1$ according as $B \neq 0$ or $B = 0$. In either case one and just one of the terms $y^{n-p} \cos px$, $y^{n-p} \sin px$ is linearly dependent on terms preceding it in sequence (1). If $h > p > 0$, on the other hand, and if

$$\Psi = y^{k-q}[A' \cos (h - p)x + B' \sin (h - p)x],$$

the product $\Psi\Omega$ has leading terms

$$\tfrac{1}{2}y^k[(AA' - BB') \cos hx + (AB' + BA') \sin hx].$$

For any $A$ and $B$ it is possible to choose values of $A'$ and $B'$ (not both zero) to make $AB' + BA' = 0$, and other values of $A'$ and $B'$ to make $AB' + BA' \neq 0$; the vanishing of $\Psi\Omega$ on $C$ means in one case that $y^k \cos hx$ and in the other

case that $y^k \sin hx$ is linearly dependent on earlier terms in (1). The corresponding facts when $p = 0$ are obvious. There are just $2(n - N) + 1$ monomials of the $n^{\text{th}}$ order in (1) which are linearly dependent on earlier terms, while the remaining $2N$ monomials of the $n^{\text{th}}$ order lead to the construction of $2N$ mixed sums of the $n^{\text{th}}$ order in the orthogonal sequence for each value of $n \geqq N$.

*If $\omega$ is of degree $2r - 1$ in $z$*, and if $\omega_1 = \psi\omega$, the degree of $\psi$ with respect to $z$ may be $2(r_1 - r) + 1$, but can be no higher. While it can not be asserted now that $\Psi$ as defined in (2) is a mixed sum in $x$ and $y$, both of the functions

$$\Psi_1(x, y) = \frac{\psi(z, y)}{(1 + z^2)^{r_1 - r + 1}}, \qquad \Psi_2(x, y) = \frac{z\psi(z, y)}{(1 + z^2)^{r_1 - r + 1}}$$

are such mixed sums. They satisfy the identities

$$\begin{aligned} \Psi_1(x, y)\Omega(x, y) &= \tfrac{1}{2}(1 + \cos x)\Omega_1(x, y), \\ \Psi_2(x, y)\Omega(x, y) &= \tfrac{1}{2} \sin x\Omega_1(x, y). \end{aligned} \tag{3}$$

*The sums $\Omega_1(1 + \cos x)$ and $\Omega_1 \sin x$ are each divisible by $\Omega$.* They are of rank $(h + 1, k)$ and order $n + 1$ if the rank and order of $\Omega_1$ are again denoted by $(h, k)$ and $n$. It is deduced at first that $h + 1 \geqq p$, $k \geqq q$. But further examination shows that the value $h = p - 1$ is inadmissible. For $\Omega_1(1 + \cos x)$ and $\Omega_1 \sin x$ would each be of rank $(p, n - p + 1)$; neither $\Psi_1$ nor $\Psi_2$ could have as leading term anything but (a constant multiple of) $y^{n-N+1}$; and so the relation $\Psi_1 \sin x = \Psi_2(1 + \cos x)$, implied by (3), would be impossible. It is true again that $h$ must have one of the values $p, p + 1, \cdots, p + n - N$. In the present case, however, $z\omega/(1 + z^2)^r = z\Omega$ is a mixed sum in $x$ and $y$; if the leading terms of $\Omega$ are $y^q(A \cos px + B \sin px)$, then those of $z\Omega = \Omega \sin x/(1 + \cos x)$ are $y^q(-B \cos px + A \sin px)$; since $A, B$ are not both zero, $y^q \sin px$ on $C$ is linearly dependent on earlier terms in (1), while the vanishing of $(A - Bz)\Omega$ on $C$ means that $y^q \cos px$ is linearly dependent on terms of lower rank. The same is true of $y^{n-p} \sin px$ and $y^{n-p} \cos px$ for any value of $n > N$. (Under the present hypothesis $\Omega = \omega/(1 + z^2)^r$ vanishes identically in $y$ for $z = \infty$, and so for $x = \pi$, which would be impossible if its leading term were $y^N$; it is certain that $p \neq 0$.) There are $2(n - N + 1)$ monomials of the $n^{\text{th}}$ order in (1) which do not meet the condition of linear independence, and the orthogonal system contains $2N - 1$ sums of the $n^{\text{th}}$ order for $n \geqq N$.

If the particular arrangement in sequence indicated in (1) for monomials of like order is not prescribed, the sums of the $n^{\text{th}}$ order in the normalized system are determined on the curve except for an orthogonal transformation among themselves, as in similar cases of orthogonal polynomials.

Recursion formulas are obtained in the usual way. If $S_{ni}(x, y)$ is one of the sums of order $n$, each of the functions $\cos xS_{ni}(x, y)$, $\sin xS_{ni}(x, y)$, $yS_{ni}(x, y)$ is linearly expressible on the curve in terms of the sums of orders $n + 1$, $n$,

and $n-1$. From these expressions it is possible to proceed to corresponding forms of the Christoffel-Darboux identity.[4]

### 3. Convergence of series of orthogonal mixed sums

The theory of convergence will be treated here only to the extent of showing by a non-trivial example that such a theory is possible of development.

Let $C$ consist of the two loops of the curve

$$1 + 2\cos 2x + 4y^2 = 0,$$

i.e. $y^2 + \cos^2 x = \frac{1}{4}$, which are contained in the strip $-\pi < x < \pi$. Here $N = 2$, and the corresponding equation in $z$ and $y$ is of the fourth degree in $z$, so that for general $n$ the orthogonal system contains four sums of the $n^{\text{th}}$ order.

Let it be noted first that a form of Bernstein's theorem is valid for mixed sums on the curve $C$. Let $S(x, y)$ be a mixed sum of the $n^{\text{th}}$ order, and suppose that $|S(x, y)| \leqq L$ on $C$. Because of the symmetry of $C$ with respect to the $y$-axis it is true also that $|S(-x, y)| \leqq L$. If

$$S_1(x, y) = \tfrac{1}{2}[S(x, y) + S(-x, y)], \qquad S_2(x, y) = \tfrac{1}{2}[S(x, y) - S(-x, y)],$$

then $|S_1(x, y)| \leqq L$, $|S_2(x, y)| \leqq L$, on $C$. With respect to $x$, $S_1(x, y)$ is a cosine sum, and $S_2(x, y)$ is a sine sum. Both $S_1(x, y)$ and $S_2(x, y)/\sin x$ are polynomials in $\cos x$ and $y$, of the $n^{\text{th}}$ (or lower) degree in these two variables together. Let

$$\sin t = 2y, \qquad \cos t = 2\cos x.$$

The functions $T_1(t) = S_1(x, y)$, $T_2(t) = S_2(x, y)/\sin x$ are trigonometric sums of the $n^{\text{th}}$ order in $t$. As $|\cos x| \leqq \frac{1}{2}$ on $C$, and hence $|\sin x| \geqq 3^{\frac{1}{2}}/2$,

$$|T_1(t)| \leqq L, \qquad |T_2(t)| \leqq 2L/3^{\frac{1}{2}}$$

for all values of $t$. Consequently

$$\left|\frac{d}{dt}T_1(t)\right| \leqq nL, \qquad \left|\frac{d}{dt}T_2(t)\right| \leqq 2nL/3^{\frac{1}{2}}.$$

If $s$ denotes length of arc on $C$,

$$ds^2 = dx^2 + dy^2 = \tfrac{1}{4}[(\sin^2 t/\sin^2 x) + \cos^2 t]\,dt^2 \geqq \tfrac{1}{4}\,dt^2,$$

so that $|dt/ds| \leqq 2$, and

$$\left|\frac{d}{ds}S_1(x, y)\right| \leqq 2nL, \qquad \left|\frac{d}{ds}[S_2(x, y)/\sin x]\right| \leqq 4nL/3^{\frac{1}{2}},$$

[4] See D. Jackson, loc. cit., pp. 235-236.

from which, together with the observation that $| d \sin x/ds | \leqq 1$, it follows for the original sum $S = S_1 + S_2$ that when $n \geqq 1$

$$\left| \frac{d}{ds} S(x, y) \right| \leqq 2nL + 4nL/3^{\frac{1}{2}} + 2L/3^{\frac{1}{2}} \leqq knL$$

on $C$, with $k = 2(1 + 3^{\frac{1}{2}})$; for brevity, $| dS/ds | \leqq 6nL$, for all $n$.

Let $f(x, y)$ be a function defined on $C$, but not necessarily defined elsewhere, and satisfying, for example, a Lipschitz condition with respect to $s$ on each loop of $C$. If

$$f_1(x, y) = \tfrac{1}{2}[f(x, y) + f(-x, y)], \qquad f_2(x, y) = \tfrac{1}{2}[f(x, y) - f(-x, y)],$$

the functions $f_1(x, y)$ and $f_2(x, y)/\sin x$, in which the denominator $\sin x$ has a positive lower bound on $C$, also satisfy Lipschitz conditions with respect to $s$. Being even functions as to their dependence on $x$, they are single-valued functions of $y$ and $\cos x$, and so are single-valued functions of $t$, which furthermore satisfy Lipschitz conditions with respect to $t$, since $ds^2 \leqq \frac{1}{4}\, dt^2/\sin^2 x \leqq dt^2/3$, $| \Delta s | \leqq | \Delta t |/3^{\frac{1}{2}}$. Consequently they can be approximately represented by trigonometric sums of the $n^{\text{th}}$ order in $t$ with errors not exceeding a constant multiple[5] of $1/n$. As a trigonometric sum of the $n^{\text{th}}$ order in $t$ is a mixed sum of the $n^{\text{th}}$ order in $x$ and $y$, and as multiplication of an approximating sum for $f_2/\sin x$ by $\sin x$ gives a mixed sum of order $n + 1$ in $x$ and $y$ approximating $f_2(x, y)$ without increase in the magnitude of the error, it follows that $f(x, y)$ can be approximately represented on $C$ by mixed sums of the $n^{\text{th}}$ order in $x$ and $y$ with errors not exceeding a constant multiple of $1/n$. Clearly theorems on trigonometric approximation involving other hypotheses on the function to be represented can be made effective on $C$ in a similar manner.

It is possible then to demonstrate the convergence of series of orthogonal mixed sums on $C$, under suitable conditions on the function to be represented and on the weight function, by a method depending on the least-square property of the development, and used elsewhere in connection with problems of similar character.[6]

With certain special types of weight function it is possible to obtain results more closely comparable with the ordinary theory of convergence of Fourier series.

In conjunction with the notation of the preceding paragraphs let $s$ be taken

---

[5] See e.g. D. Jackson, *The Theory of Approximation*, American Mathematical Society Colloquium Publications, vol. 11, 1930, p. 2.

For theorems on approximation by means of mixed sums over a two-dimensional region, which can be used as basis for an alternative demonstration here, see E. L. Mickelson. *On the approximate representation of a function of two variables*, Transactions of the American Mathematical Society, vol. 33 (1931), pp. 759–781; pp. 769–770.

[6] See e.g. D. Jackson, *Certain problems of closest approximation*, Bulletin of the American Mathematical Society, vol. 39 (1933), pp. 889–906; pp. 898–903.

as increasing with $t$, and let the weight function associated with $ds$ for integration on $C$ be taken as

$$\rho(x, y) = \left[\frac{y^2}{\sin^2 x} + \cos^2 x\right]^{-\frac{1}{2}} = \frac{dt}{ds}.$$

If $F(x, y)$ is any function such that $F(-x, y) = -F(x, y)$, $\int_C \rho F\, ds = 0$ when the integration is extended over both loops of the curve; if $F(-x, y) = F(x, y) = \Phi(t)$,

$$\int_C \rho(x, y)F(x, y)\, ds = 2\int_0^{2\pi} \Phi(t)\, dt,$$

since the point $(x, y)$ traces one or the other loop of the curve when $t$ goes from 0 to $2\pi$, according as $x$ in the relation $\cos x = \frac{1}{2}\cos t$ is taken positive or negative.

Let $S_{01}(x, y) = 1/(4\pi)^{\frac{1}{2}}$, and for $n \geqq 1$ let $S_{n1}(x, y)$ and $S_{n2}(x, y)$ be expressions for $\cos nt/(2\pi)^{\frac{1}{2}}$ and $\sin nt/(2\pi)^{\frac{1}{2}}$ as mixed sums in $x$ and $y$. These functions are normalized and orthogonal to each other for integration over $C$ with weight function $\rho$. Let $U_n(t)$, $n = 0, 1, 2, \cdots$, and $V_n(t)$, $n = 1, 2, \cdots$, be normalized orthogonal trigonometric sums[7] over the interval $(0, 2\pi)$ with respect to $\sin^2 x = \frac{7}{8} - \frac{1}{8}\cos 2t$ as weight function. The combinations $S_{n3}(x, y) = \sin xU_{n-1}(t)/2^{\frac{1}{2}}$, $S_{n4}(x, y) = \sin xV_{n-1}(t)/2^{\frac{1}{2}}$ as mixed sums of the $n^{\text{th}}$ order in $x$ and $y$ are normalized and orthogonal over $C$ with respect to $\rho$. Any sum $S_{n1}$ or $S_{n2}$ is orthogonal to any sum $S_{n3}$ or $S_{n4}$, because one is even and the other odd with respect to $x$. So these sums $S_{n1}, \cdots, S_{n4}$ constitute the orthogonal system[8] for the curve $C$ and weight $\rho$.

*The sums $S_{n1}(x, y), \cdots, S_{n4}(x, y)$ are uniformly bounded on $C$ as $n$ becomes infinite.* The functions $\cos nt$, $\sin nt$ are of course bounded; and the same is true[9] of $U_n(t)$, $V_n(t)$, since the weight function $\sin^2 x$ is a positive trigonometric sum in $t$. With modifications in the reasoning appropriate to the somewhat greater complexity of the problem, the boundedness of the orthogonal sums can be used in connection with the representation of the partial sum of the series by means of the Christoffel-Darboux formula for the treatment of convergence in the same manner as in the case of orthogonal polynomials[10] or orthogonal trigonometric sums[11] in one variable.

When the property of boundedness has been established for the normalized orthogonal sums belonging to a particular weight function, it can be extended

---

[7] See D. Jackson, *Orthogonal trigonometric sums*, Annals of Mathematics, (2), vol. 34 (1933), pp. 799–814.

[8] A corresponding observation has been used by Mr. Fulton Koehler in another connection: see Bulletin of the American Mathematical Society, vol. 43 (1937), p. 772, Abstract No. 402.

[9] See D. Jackson, *Orthogonal trigonometric sums*, loc. cit., pp. 805–807.

[10] See e. g. D. Jackson, *Series of orthogonal polynomials*, Annals of Mathematics, (2), vol. 34 (1933), pp. 527–545.

[11] *Orthogonal trigonometric sums*, loc. cit.

to those corresponding to any weight function obtained from the first by multiplying it by a mixed sum which is everywhere positive on the curve.

## 4. Double trigonometric sums

In a double trigonometric sum, the terms

$$\cos px \cos qy,\ \cos px \sin qy,\ \sin px \cos qy,\ \sin px \sin qy \tag{4}$$

will be said to be of rank $(p, q)$. Ranks will be compared as higher and lower in accordance with the convention already used. The highest rank found among the terms of a sum will be the rank of the sum, and the terms having this rank will be the leading terms. If the rank is $(p, q)$, the order of the sum is $p + q$. When there is occasion to recognize an order of precedence among the terms (4), they will be taken in the order indicated. For the initial application of the process of orthogonalization the monomials will be taken in the sequence

$$\begin{aligned} &1,\ \cos x,\ \sin x,\ \cos y,\ \sin y,\ \cos 2x,\ \sin 2x, \\ &\cos x \cos y,\ \cos x \sin y,\ \sin x \cos y,\ \sin x \sin y,\ \cos 2y,\ \sin 2y,\ \cdots . \end{aligned} \tag{5}$$

There are $4n$ monomials of order $n$ when $n > 0$.

*The order of a product of two double trigonometric sums is not necessarily the sum of the orders of the factors.* For example.

$$(\cos px \cos qy + \sin px \sin qy)(\cos px \cos qy - \sin px \sin qy)$$
$$= \cos (px - qy) \cos (px + qy) = \tfrac{1}{2}(\cos 2px + \cos 2qy).$$

If a sum of rank $(p, q)$ is multiplied by one of rank $(r, s)$, the order of the product can not of course be higher than $p + q + r + s$, and the rank of the product can not be higher than $(p + r, q + s)$. An examination will presently be made of the special circumstances under which the rank of the product can be lower. If a sum of rank $(p, q)$ is multiplied by any one of the four *monomials* $\cos rx \cos sy$, $\cos rx \sin sy$, $\sin rx \cos sy$, $\sin rx \sin sy$, the rank of the product is $(p + r, q + s)$ in each case.

A closely related question which is important in studying the make-up of a system of double trigonometric sums orthogonal on a curve is whether, if a sum of rank $(p, q)$ vanishes identically on a specified curve, every monomial in the sequence (5) which is of order higher than $p$ in $x$ and at the same time of order higher than $q$ in $y$ is on this curve linearly dependent on terms preceding it in the sequence, and so to be left out of account in the formation of successive members of the orthogonal system. This question will be discussed before that of the preceding paragraph, incompletely to be sure, but far enough to permit a form of definite statement.

Suppose that on a curve $K$ a double trigonometric sum $\Omega(x, y)$, of rank $(p, q)$, with leading terms

$$A \cos px \cos qy + B \cos px \sin qy + C \sin px \cos qy + D \sin px \sin qy,$$

vanishes identically, $p > 0$, $q > 0$; some, but not all, of the coefficients $A$, $B$, $C$, $D$ may be zero. The product

$$4\Omega(x, y)(\alpha \cos rx \cos sy + \beta \cos rx \sin sy + \gamma \sin rx \cos sy + \delta \sin rx \sin sy),$$

with $r > 0$, $s > 0$, has leading terms

$$\begin{aligned}(6)\quad &(A\alpha - B\beta - C\gamma + D\delta) \cos (p + r)x \cos (q + s)y \\ &+ (B\alpha + A\beta - D\gamma - C\delta) \cos (p + r)x \sin (q + s)y \\ &+ (C\alpha - D\beta + A\gamma - B\delta) \sin (p + r)x \cos (q + s)y \\ &+ (D\alpha + C\beta + B\gamma + A\delta) \sin (p + r)x \sin (q + s)y,\end{aligned}$$

if this combination of terms is not identically zero. It is possible to choose $\alpha$, $\beta, \gamma, \delta$ so as to reduce any one of these coefficients to 1 and the rest to 0, if the determinant

$$\Delta = \begin{vmatrix} A & -B & -C & D \\ B & A & -D & -C \\ C & -D & A & -B \\ D & C & B & A \end{vmatrix}$$

is different from zero. That is to say, if $\Delta \neq 0$ each of the monomials

$$\cos (p + r)x \cos (q + s)y, \quad \cos (p + r)x \sin (q + s)y,$$
$$\sin (p + r)x \cos (q + s)y, \quad \sin (p + r)x \sin (q + s)y$$

is linearly dependent on monomials of lower rank when $\Omega = 0$. If $p + q = N$, and if $p + q + r + s = n$ is given, $r$ can have any of the values $1, 2, \cdots, n - N - 1$, and (at least) $4(n - N - 1)$ monomials of the $n^{\text{th}}$ order are linearly dependent on earlier terms. The number of sums of the $n^{\text{th}}$ order in the orthogonal system does not exceed $4n - 4(n - N - 1) = 4N + 4$, which is independent of $n$.

For $r = 0$, $s > 0$ the product

$$2\Omega(x, y)(\alpha \cos sy + \beta \sin sy)$$

has leading terms

$$\begin{aligned}(7)\quad &(A\alpha - B\beta) \cos px \cos (q + s)y + (B\alpha + A\beta) \cos px \sin (q + s)y \\ &+ (C\alpha - D\beta) \sin px \cos (q + s)y + (D\alpha + C\beta) \sin px \sin (q + s)y\end{aligned}$$

if these terms do not all vanish. Here arbitrary values can be given to the last two coefficients by suitable choice of $\alpha$ and $\beta$, unless $C = D = 0$, in which case $A$ and $B$ are not both zero, and arbitrary values can be given to the first two coefficients. So at least two of the monomials in (7) are linearly dependent on earlier terms in (5) on the curve $K$. A similar argument, with slight though

not purely formal modification, applies if $r > 0$, $s = 0$. The upper bound $4N + 4$ is thereby reduced to $4N$.

Combination of rows with rows in the multiplication of the determinant $\Delta$ by itself gives for $\Delta^2$ the expression

$$\begin{vmatrix} A^2+B^2+C^2+D^2 & 0 & 0 & 2(AD-BC) \\ 0 & A^2+B^2+C^2+D^2 & -2(AD-BC) & 0 \\ 0 & -2(AD-BC) & A^2+B^2+C^2+D^2 & 0 \\ 2(AD-BC) & 0 & 0 & A^2+B^2+C^2+D^2 \end{vmatrix}$$

$$= [(A^2 + B^2 + C^2 + D^2)^2 - 4(AD - BC)^2]^2.$$

The vanishing of $\Delta$ accordingly means that

$$A^2 + B^2 + C^2 + D^2 \pm 2(AD - BC) = (A \pm D)^2 + (B \mp C)^2 = 0,$$

$$C = \pm B, \qquad D = \mp A.$$

The leading terms of $\Omega(x, y)$ then have the form

$$A \cos(px \pm qy) + B \sin(px \pm qy),$$

the $\pm$ sign being the same in both terms. In every other case the orthogonal system contains not more than $4N$ sums of the $n^{\text{th}}$ order for any $n$. The same conclusion holds naturally if $x$ and $y$ are interchanged in the definition of rank, i.e. if the terms which are of highest order in $x$ among the terms of maximum order in the two variables together do not have the indicated special form.

If the leading terms of $\Omega(x, y)$ are $A \cos qy + B \sin qy$, with $p = 0$, $q = N$, the leading terms of

$$2\Omega(x, y)(\alpha \cos rx \cos sy + \beta \cos rx \sin sy + \gamma \sin rx \cos sy + \delta \sin rx \sin sy),$$

$r > 0$, $s > 0$, are

$$(A\alpha - B\beta) \cos rx \cos(q + s)y + (B\alpha + A\beta) \cos rx \sin(q + s)y$$
$$+ (A\gamma - B\delta) \sin rx \cos(q + s)y + (B\gamma + A\delta) \sin rx \sin(q + s)y$$

if any of these terms are present. Arbitrary values can be assigned to all four coefficients by choice of $\alpha$, $\beta$, $\gamma$, $\delta$, without any restriction on $A$ and $B$ except that they do not both vanish; each of the monomials involved is linearly dependent on earlier members of the sequence (5); and the orthogonal system on $K$ contains not more than $4N + 4$ sums of the $n^{\text{th}}$ order. Special consideration of the cases $r = 0$, $s > 0$ and $r > 0$, $s = 0$ again reduces this upper bound to $4N$. Similar reasoning obviously applies if $p = N$, $q = 0$.

The discussion is left unfinished for the time being as regards the special cases ruled out above.

To return to the question of the order of a product, let $T_1(x, y)$ and $T_2(x, y)$

be any two double trigonometric sums of ranks $(p, q)$ and $(r, s)$, with leading terms

$$A \cos px \cos qy + B \cos px \sin qy + C \sin px \cos qy + D \sin px \sin qy$$

and

$$\alpha \cos rx \cos sy + \beta \cos rx \sin sy + \gamma \sin rx \cos sy + \delta \sin rx \sin sy.$$

The leading terms of the product $T_1T_2$ are given except for a factor $\frac{1}{4}$ by the expression (6), if that expression does not reduce to zero. For the simultaneous vanishing of the four coefficients in (6) with values of $\alpha, \beta, \gamma, \delta$ not all zero it is necessary that $\Delta = 0$. Similarly, if the coefficients are regarded as linear combinations of $A, B, C, D$ it is seen that the corresponding determinant in terms of $\alpha, \beta, \gamma, \delta$ must be zero. *The rank of the product is* $(p + r, q + s)$, *unless both factors have leading terms of the special form previously discussed.* This is on the assumption that $p, q, r, s$ are all positive. If $pqrs = 0$ the rank of the product is $(p + r, q + s)$ without further restriction on the coefficients.

The theory of orthogonal systems can now be extended from mixed sums to double trigonometric sums with limitations corresponding to the points of difference that have been noted.

Let $T(x, y)$ be a double trigonometric sum which is of order $r$ in $x$ and of order $s$ in $y$. Let

$$z = \tan \frac{x}{2}, \qquad w = \tan \frac{y}{2}.$$

Then $T(x, y)$ is of the form $P(z, w)/[(1 + z^2)^r(1 + w^2)^s]$, where the numerator is a polynomial in $z$ and $w$ of degree $2r$ at most in $z$ and of degree $2s$ at most in $w$. And any fraction so constituted is a double trigonometric sum of corresponding orders in $x$ and $y$.

Let $K$ be a curve in the $(x, y)$ plane, restricted for simplicity to the period square $-\pi < x < \pi$, $-\pi < y < \pi$, and forming a part of the locus of an equation $\Omega_0(x, y) = 0$, where $\Omega_0$ is a double trigonometric sum. The corresponding curve $K'$ in the $(z, w)$ plane is a part (or the whole) of an algebraic locus. Let $\omega(z, w)$ be the polynomial of lowest degree vanishing identically on $K'$. If $\omega$ is of even degree in each variable, $2r$ with respect to $z$ and $2s$ with respect to $w$, and if

$$\Omega(x, y) = \frac{\omega(z, w)}{(1 + z^2)^r(1 + w^2)^s},$$

$\Omega$ is a double trigonometric sum vanishing on $K$, and every double trigonometric sum which vanishes identically on $K$ is divisible by $\Omega$, as may be seen by reasoning similar to that used in connection with mixed sums. If $\Omega$ is of rank $(p, q)$ and of order $p + q = N$, and if its leading terms are not of the form recognized above as exceptional, a monomial of rank $(p', q')$ and order $n$ in the sequence (5) is on $K$ linearly dependent on monomials preceding it in the sequence if

$p' > p$, $q' > q$, and only if $p' \geqq p$, $q' \geqq q$. It has been observed that the number of sums of the $n^{\text{th}}$ order in the orthogonal system on $K$ can not exceed $4N$ for $n > N$. Further examination of the cases $p' = p$ and $q' = q$ shows that the number is $4N$ exactly. If the degree of $\omega$ in either variable is odd, supplementary considerations are called for as in the case of mixed sums.

It is possible then to work further along lines corresponding to those followed in the earlier sections, for the derivation of recursion formulas and Christoffel-Darboux identities, and the development of an illustrative theory of convergence associated, for example, with the curve

$$\cos^2 x + \cos^2 y = \tfrac{1}{4}, \qquad 2\cos 2x + 2\cos 2y + 3 = 0.$$

THE UNIVERSITY OF MINNESOTA,
MINNEAPOLIS, MINNESOTA.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ON SUMS OF POSITIVE INTEGRAL $k^{\text{th}}$ POWERS

BY H. DAVENPORT AND P. ERDÖS

(Received February 20, 1939)

1. Let $k \geqq 3$ be an integer. Let $N_s^{(k)}(n)$ denote the number of integers not exceeding $n$ that are representable as the sum of $s$ positive integral $k^{\text{th}}$ powers. We are concerned in this paper with inequalities of the form

$$N_s^{(k)}(n) > n^{\alpha}, \qquad \alpha = \alpha(k, s),$$

valid for all large $n$. Such inequalities are of great importance in the application of the Hardy-Littlewood method to Waring's Problem.

Until recently, practically the only such inequality known was that of Hardy and Littlewood[1]

$$N_s^{(k)}(n) > n^{\alpha_1 - \epsilon}, \qquad \alpha_1 = 1 - \left(1 - \frac{2}{k}\right)\left(1 - \frac{1}{k}\right)^{s-2}, \tag{1}$$

valid for any $\epsilon > 0$ and $n > n_0(\epsilon)$.[2]

This has been improved upon independently by the two authors of the present paper, using different methods. We give here an account of the method of Erdös, with modifications due to Davenport.[3]

2. DEFINITION. *$s$ positive numbers $\lambda_1, \cdots, \lambda_s$ satisfying $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_s$ are called admissible exponents for $k^{\text{th}}$ powers if the number of solutions of*

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k \tag{2}$$

*in integers subject to*

$$P^{\lambda_1} < x_1, y_1 < 2P^{\lambda_1}; \cdots; \qquad P^{\lambda_s} < x_s, y_s < 2P^{\lambda_s} \tag{3}$$

*is $O(P^{\lambda_1 + \cdots + \lambda_s + \epsilon})$ as $P \to \infty$, for any $\epsilon > 0$.*

It is easily seen[4] that if $\lambda_1, \cdots, \lambda_s$ are admissible exponents for $k^{\text{th}}$s, power then

$$N_s^{(k)}(n) > n^{\alpha - \epsilon}, \qquad \alpha = \frac{\lambda_1 + \cdots + \lambda_s}{k\lambda_1}, \tag{4}$$

for any $\epsilon > 0$ and $n > n_0(\epsilon)$.

---

[1] See, for example, Landau, *Vorlesungen über Zalentheorie*, (Leipzig, 1927), 1, Satz 348.

[2] For $s = 2$, Erdös and Mahler (*Journal London Math. Soc.*, 13 (1938), pp. 134–139) have proved that $N_2^{(k)}(n) > cn^{2/k}$, where $c > 0$ depends only on $k$.

[3] The results of Davenport are in course of publication in the *Proc. Royal Soc.* An account of the particular case $k = 4$, $s = 3$ has appeared in the *Comptes Rendus*, 207 (1938), p. 1366.

[4] A formal proof is given in Davenport's paper in *Proc. Royal Soc.*

In what follows, $c_1, c_2, \cdots$ denote positive numbers depending only on $k$ and $s$.

THEOREM 1. *Let* $\theta = 1 - k^{-1}$. *Then* $1, \lambda, \lambda\theta, \lambda\theta^2, \cdots, \lambda\theta^{s-2}$ *are admissible exponents for* $k^{\text{th}}$ *powers, provided* $\lambda$ *satisfies*

$$k\lambda - (k-1) \leqq \lambda\theta^{s-2}. \tag{5}$$

PROOF. (1) Suppose that $s = 2$. It is well known that the number of representations of an integer $m$ as $y_1^k + y_2^k$ with positive integral $y_1, y_2$ is $O(m^\epsilon)$, for any $\epsilon > 0$. Hence any *two* positive numbers are admissible exponents for $k^{\text{th}}$ powers. Thus the theorem is true for $s = 2$.

(2) Suppose that $s \geqq 3$, and that the theorem is true with $s-1$ in place of $s$.

Let $x_1, \cdots, x_s, y_1, \cdots, y_s$ satisfy (2) and (3), where $\lambda_1 = 1, \lambda_2 = \lambda, \lambda_3 = \lambda\theta, \cdots, \lambda_s = \lambda\theta^{s-2}$. Since

$$|x_1^k - y_1^k| > P^{k-1}|x_1 - y_1|,$$

we have

$$|x_1 - y_1| < c_1 \frac{P^{k\lambda}}{P^{k-1}} \leqq c_1 P^{\lambda\theta^{s-2}},$$

by (5). Hence the number of possible pairs $x_1, y_1$ is $O(P^{1+\lambda\theta^{s-2}})$. The number of possible sets of values for $x_1, y_1, x_2, x_3, \cdots, x_{s-1}$ is therefore $O(P^{1+\lambda+\lambda\theta+\ldots+\lambda\theta^{s-2}})$. For fixed values of these variables, (2) has the form

$$\begin{aligned} A &= y_2^k + y_3^k + \cdots + y_s^k - x_s^k \\ &= y_2^k + O(P^{k\lambda\theta}), \end{aligned}$$

where $A$ is fixed. This has only $O(1)$ solutions $y_2$ with $P^\lambda < y_2 < 2P^\lambda$, since

$$(y_2+1)^k - y_2^k > (P^\lambda)^{k-1} = P^{k\lambda\theta}.$$

For fixed $y_2$, the argument can be repeated (if $s \geqq 4$) and shows that there are only $O(1)$ possibilities for $y_3$, and so on generally. Finally, (2) takes the form

$$B = y_s^k - x_s^k,$$

which has only $O(P^\epsilon)$ solutions, unless $B = 0$. Hence the total number of solutions of (2), subject to (3), with $x_s \neq y_s$ is $O(P^{1+\lambda+\lambda\theta+\ldots+\lambda\theta^{s-2}+\epsilon})$.

For the solutions with $x_s = y_s$, we observe that, since

$$k\lambda - (k-1) \leqq \lambda\theta^{s-2} \leqq \lambda\theta^{s-3},$$

$1, \lambda, \lambda\theta, \cdots, \lambda\theta^{s-3}$ are admissible exponents for $k^{\text{th}}$ powers (by the case $s-1$ of the theorem). Hence the number of solutions with $x_s = y_s$ is

$$O(P^{1+\lambda+\lambda\theta+\ldots+\lambda\theta^{s-3}+\epsilon+\lambda\theta^{s-2}}).$$

This establishes Theorem 1.

COROLLARY. *For any $\epsilon > 0$, and $n > n_0(\epsilon)$,*

$$(6)\quad N_s^{(k)}(n) > n^{\alpha_2-\epsilon}, \qquad \alpha_2 = 1 - \frac{1-\frac{1}{k}}{1-\frac{1}{k}\left(1-\frac{1}{k}\right)^{s-2}}\left(1-\frac{2}{k}\right)\left(1-\frac{1}{k}\right)^{s-2}.$$

PROOF. Taking $\lambda = (k-1)/(k-\theta^{s-2})$, we have

$$\frac{1}{k}(1+\lambda+\lambda\theta+\cdots+\lambda\theta^{s-2}) = \frac{1}{k}\left(1+\frac{k-1}{k-\theta^{s-2}}\,\frac{1-\theta^{s-1}}{1-\theta}\right)$$

$$= 1 - \frac{1-\frac{1}{k}}{1-\frac{1}{k}\left(1-\frac{1}{k}\right)^{s-2}}\left(1-\frac{2}{k}\right)\left(1-\frac{1}{k}\right)^{s-2},$$

on simplification.

Comparing (1) with (6), it is plain that $\alpha_2 > \alpha_1$ (provided $s > 2$).

3. THEOREM 2. *$1,\ 1-\frac{1}{k^2},\ 1-\frac{1}{k}-\frac{1}{k^2}$ are admissible exponents for $k^{\text{th}}$ powers.*

PROOF. Let $x_1, y_1, z_1, x_2, y_2, z_2$ satisfy

$$(7)\quad x_1^k + y_1^k + z_1^k = x_2^k + y_2^k + z_2^k,$$

$$(8)\quad P < x_1, x_2 < 2P, \qquad P^{1-k^{-2}} < y_1, y_2 < 2P^{1-k^{-2}},$$
$$P^{1-k^{-1}-k^{-2}} < z_1, z_2 < 2P^{1-k^{-1}-k^{-2}}.$$

The number of solutions of (7), (8) with $x_1 = x_2$ is

$$O(P^{1+1-k^{-2}+1-k^{-1}-k^{-2}+\epsilon}).$$

Hence we need only consider solutions with $x_2 > x_1$. By a similar argument, we can also suppose that $z_1 \neq z_2$.

Writing $x_2 = x_1 + t$, (7) becomes

$$(9)\quad (x_1+t)^k - x_1^k + y_2^k - y_1^k = z_1^k - z_2^k.$$

Plainly

$$tP^{k-1} < (x_1+t)^k - x_1^k < y_1^k + z_1^k < 2(2P^{1-k^{-2}})^k,$$

whence

$$(10)\quad 0 < t < c_2 P^{1-k^{-1}}.$$

For fixed $t, y_1, y_2$, (9) has the form

$$(11)\quad (x_1+t)^k - x_1^k + A = O(P^{k-1-k^{-1}}).$$

Since

$$\{(x_1+1+t)^k - (x_1+1)^k\} - \{(x_1+t)^k - x_1^k\} > c_3 t P^{k-2},$$

the number of values of $x_1$ satisfying (11) is

$$O\left(\frac{P^{k-1-k^{-1}}}{tP^{k-2}}+1\right)=O\left(\frac{P^{1-k^{-1}}}{t}+1\right).$$

Hence the number of sets $x_1$, $t$, $y_1$, $y_2$ satisfying (9), (10), (8) is

$$O\left(P^{2(1-k^{-2})}\sum_{0<t<c_2P^{1-k^{-1}}}\left(\frac{P^{1-k^{-1}}}{t}+1\right)\right)=O(P^{2(1-k^{-2})+(1-k^{-1})+\epsilon}).$$

Also, for fixed values of these variables, (9) has only $O(P^{\epsilon})$ solutions in $z_1$, $z_2$ with $z_1 \neq z_2$.

Hence the number of solutions of (7), (8) is

$$O(P^{1+(1-k^{-2})+(1-k^{-1}-k^{-2})+\epsilon}),$$

which proves the theorem.

COROLLARY. *For any* $\epsilon > 0$ *and* $n > n_0(\epsilon)$,

$$N_3^{(k)}(n) > n^{\alpha_3-\epsilon}, \qquad \alpha_3 = \frac{3}{k}-\frac{k+2}{k^3}.$$

The value of $\alpha_2$ given by the Corollary to Theorem 1 in the case $s = 3$ is

$$\alpha_2 = \frac{3}{k}-\frac{k+1}{k(k^2-k+1)}.$$

It is easily verified that $\alpha_3 > \alpha_2$.

**4.** The results above obtained for $N_s^{(k)}(n)$ are not as precise as those of Davenport when $k \leqq 5$, but are at any rate more precise when $k \geqq 6$ and $s = 3$. It may be remarked that the case $k = 4$, $s = 4$ of the Corollary to Theorem 1, namely

$$N_4^{(4)}(n) > n^{(83/110)-\epsilon},$$

is sufficient for the proof that $G(4) = 16$, though not for the further results announced by Davenport.[5]

VICTORIA UNIVERSITY, MANCHESTER, ENGLAND, AND
INSTITUTE FOR ADVANCED STUDY, PRINCETON, N. J.

---

[5] *Comptes Rendus*, loc. cit.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ON POLYNOMIALS WITH ONLY REAL ROOTS[1]

BY P. ERDÖS AND T. GRÜNWALD

(Received December 19, 1938)

## 1

We start from some well known elementary properties of the parabola of second order. Denote its axis by $t$, the vertex by $C$; in any point $C_1$ of the axis draw the perpendicular to it, meeting the parabola at $A_1$ and $A_2$ respectively. If the foot of the perpendiculars from $A_1$ and $A_2$ to the tangent at the vertex are denoted by $B_1$ and $B_2$ respectively and the point of intersection of the tangents at $A_1$ and $A_2$ by $T$ (Fig. 1) then we have

$$\overline{TC_1} = 2\overline{CC_1}$$

and

$$F = \tfrac{2}{3}\Delta A_1A_2T = \tfrac{2}{3}\,\text{rect}\,A_1A_2B_2B_1,$$

where $F$ denotes the area of the parabola above $\overline{A_1A_2}$.

It is evident that these properties do not hold for polynomials of degree $n > 2$. We shall now enquire if for $n > 2$ the ratio of the above distances and areas remains between certain limits.

Let $g(x)$ be a polynomial of degree $n$ with $n \geqq 2$, $p$ and $q$ $(p < q)$ two consecutive real roots and suppose $g(x)$ to be positive throughout the interval $(p, q)$. Let $g(x)$ assume its maximum value in $(p, q)$ at $b$. The tangents at $p$ and $q$ meet at a point $T$ with $t$ as ordinate. In general $t > 0$ and for $g'(p) = g'(q) = 0$ we assign to $t$ the value 0. Throughout this paper $\Delta pqT$ will be referred to as the *"tangential triangle"*; its area is given by $\frac{1}{2}(q - p)t$. The part of the curve between $p$ and $q$ may be included in the *"tangential rectangle"* of area $(q - p)g(b)$, and $\int_p^q g(x)\,dx$ defines the *"area of the curve."*

The ratio $t/g(b)$ and that of the *area of the tangential triangle to the area of the curve* which, in the case $n = 2$ take the values 2 and 3/2 respectively, may in the general case, assume any value. They may be less then any number we may choose, however small; they may even equal 0, e.g. if $p$ is a multiple root, i.e. if $g'(p) = 0$ and thus also $t = 0$. But they may also be larger than any number we may choose, however large; as, e.g. in the case $g(x) = 1 - x^{2n}$. Here $p = -1$, $q = +1$, $b = 0$, $g(0) = 1$, $t = 2n$, hence

$$t/g(0) = 2n \quad \text{and} \quad \frac{q-p}{2}\,t \Big/ \int_p^q g(x)\,dx > 2n/2 = n.$$

[1] In this paper we consider only polynomials with real coefficients.

This example at the same time illustrates that the ratio of *area of the curve to the area of the tangential rectangle* may approach unity as close as we like. But, as the example $g(x) = (1 - x^2)^n$ shows, the same ratio may assume values less then any preassigned number however small.

Thus we see that, for *any* polynomial the above ratios cannot be enclosed between definite limits (trivial ones disregarded). *But for polynomials with only real roots we proved the following theorems.*

THEOREM I. $t \leqq 2g(b)$.

THEOREM II. *The area of the curve is greater than or equal to* $\frac{2}{3}$ *the area of the tangential triangle*:

$$\int_p^q g(x)\,dx \geqq \frac{2}{3}\left(\frac{q-p}{2}\,t\right).$$

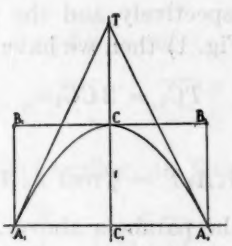


FIG. 1

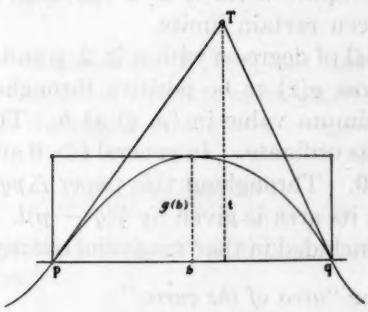


FIG. 2

THEOREM III. *The area of the curve is less than or equal to* $\frac{2}{3}$ *the area of the tangential rectangle*:

$$\int_p^q g(x)\,dx \leqq \tfrac{2}{3}[(q-p)g(b)].$$

*In all cases equality holds only for* $n = 2$.

Theorem I and its proof under 2 is due to G. Szekeres.[2]

[2] Oral communication.

Theorems II and III may be written

$$\frac{2}{3}\left(\frac{q-p}{2}t\right) \leqq \int_p^q g(x)\,dx \leqq \frac{2}{3}[(q-p)g(b)].$$

Hence

$$\frac{2}{3}\left(\frac{q-p}{2}t\right) \leqq \frac{2}{3}[(q-p)g(b)],$$

*i.e. the area of the tangential triangle is less than or equal to the area of the tangential rectangle.*

From this inequality we immediately obtain

$$t \leqq 2g(b)$$

i.e. *theorem I is a consequence of II and III.* Nevertheless we give Szekeres's proof as it leads to the result immediately and by very simple means.

In 3 we prove two lemmas required and in 4 and 5 our theorems II and III.

## 2. Proof of theorem I due to G. Szekeres

Let

$$g(x) = A(x-a_1)(x-a_2)\cdots(x-a_n) \qquad (n \geqq 2),$$

where for the real $a_i$'s

$$a_1 \geqq a_2 \geqq \cdots \geqq a_{k-1} > a_k \geqq \cdots \geqq a_n. \qquad (2 \leqq k \leqq n).$$

Assume

$$p = a_k \quad \text{and} \quad q = a_{k-1}.$$

At a certain $b_{k-1}$ in $(a_k, a_{k-1})$ $g'(x)$ vanishes and, if we suppose $g(x)$ to be positive in $(a_k, a_{k-1})$, the function assumes at $b_{k-1}$ its maximum. Thus $g(x) > 0$ $(a_k < x < a_{k-1})$, $b = b_{k-1}$ and if we denote by $T_{k-1}$ the point of intersection of the tangents at $a_{k-1}$ and $a_k$, we have to prove

$$t_{k-1} \leqq 2g(b_{k-1}),$$

where $t_{k-1}$ denotes the ordinate of $T_{k-1}$.

If one of the values $g'(a_{k-1})$ and $g'(a_k)$ equals 0 then $t_{k-1} = 0$ and our theorem is a trivial one. (The same holds for $g'(a_{k-1}) = g'(a_k) = 0$ for in this case, according to our definition, $t_{k-1} = 0$). For $n = 2$ we have, by simple computation $t_{k-1} = 2g(b_{k-1})$. Hence we may assume

(1) $$g'(a_{k-1})g'(a_k) \neq 0 \quad \text{and} \quad n \geqq 3.$$

By easy computation

$$t_{k-1} = (a_{k-1}-a_k)\cdot\frac{|g'(a_{k-1})|\,|g'(a_k)|}{|g'(a_{k-1})|+|g'(a_k)|} = \frac{a_{k-1}-a_k}{2}\cdot\frac{2}{\dfrac{1}{|g'(a_{k-1})|}+\dfrac{1}{|g'(a_k)|}}$$

i.e.

$$t_{k-1} \leqq \frac{a_{k-1} - a_k}{2} (|g'(a_{k-1})||g'(a_k)|)^{\frac{1}{2}} = s_{k-1}$$

since the harmonic mean of two positive numbers is not greater than their geometric mean.
Now we prove

$$s_{k-1} < 2g\left(\frac{a_{k-1} + a_k}{2}\right)$$

by which, properly said, we prove more than is contained in theorem I; for we prove that $t_{k-1}$ is less that the double of the value assumed at the bisection of the interval $(a_k , a_{k-1})$.

Without loss of generality we may suppose

$$a_{k-1} = 1 \quad \text{and} \quad a_k = -1.$$

Hence, by (1), according to which $-1$ and $+1$ are simple roots, we have

$$|a_i| > 1 \qquad (i = 1, 2, \cdots k-2, k+1, \cdots, n) \tag{2}$$

and

$$s_{k-1} = (|g'(-1)||g'(1)|)^{\frac{1}{2}}, \qquad \frac{a_{k-1} + a_k}{2} = 0.$$

$$|g'(1)| = |A(1 - a_1)(1 - a_2) \cdots (1 - a_{k-2})(1 + 1)(1 - a_{k+1}) \cdots (1 - a_n)|$$
$$= 2|A(a_1 - 1)(a_2 - 1) \cdots (a_{k-2} - 1)(a_{k+1} - 1) \cdots (a_n - 1)|.$$

$$|g'(-1)| = 2|A(a_1 + 1)(a_2 + 1) \cdots (a_{k-2} + 1)(a_{k+1} + 1) \cdots (a_n + 1)|.$$

i.e. by (1) and (2)

$$s_{k-1} = (4A^2(a_1^2 - 1)(a_2^2 - 1) \cdots (a_{k-2}^2 - 1)(a_{k+1}^2 - 1) \cdots (a_n^2 - 1))^{\frac{1}{2}}$$
$$< 2(A^2 a_1^2 a_2^2 \cdots a_{k-2}^2 a_{k+1}^2 \cdots a_n^2)^{\frac{1}{2}} = 2|Aa_1 a_2 \cdots a_{k-2} a_{k+1} \cdots a_n| = 2g(0).$$

Q.e.d.

## 3

Suppose that the roots $c_1 , c_2 , \cdots , c_\nu$ of the polynomial of degree $\nu$ ($\nu \geqq 3$)

$$h(x) = C(x - c_1)(x - c_2)(x - c_3) \cdots (x - c_\nu)$$

are all real; $c_1 > c_2 > c_3 \geqq \cdots \geqq c_\nu$, i.e. the two greatest roots are simple. Further let $h(x)$ be negative in $(c_2 , c_1)$ and positive in $(c_3 , c_2)$ i.e. $C > 0$. Then we prove

LEMMA 1. *If* $c_2 - c_3 \leqq c_1 - c_2$, *then* $\int_{c_3}^{c_1} h(x)\,dx \leqq 0$ and

LEMMA 2. *If*

$$\frac{1}{c_2 - c_3} + \frac{1}{c_2 - c_4} + \cdots + \frac{1}{c_2 - c_\nu} \leqq \frac{1}{c_1 - c_2},$$

*then*

$$\int_{c_3}^{c_1} h(x)\,dx \geqq 0.$$

*In both lemmas equality holds only for* $\nu = 3$ *with* $c_2 - c_3 = c_1 - c_2$.

Without loss of generality we may assume

$$c = 1, \qquad c_1 = 1, \qquad c_2 = 0.$$

Put $\gamma_i = -c_i$ for $3 \leqq i \leqq \nu$. Then

$$h(x) = (x - 1)x(x + \gamma_3)(x + \gamma_4) \cdots (x + \gamma_\nu)$$

and

$$0 < \gamma_3 \leqq \gamma_4 \leqq \cdots \leqq \gamma_\nu. \tag{3}$$

PROOF OF LEMMA 1.

We have to prove that for $\gamma_3 \leqq 1$, $\int_{-\gamma_3}^{1} h(x)\,dx \leqq 0$. It will be sufficient to prove that

$$|h(-x)| \leqq |h(x)|. \qquad (0 < x < \gamma_3 (\leqq 1)).$$

By (3) and $\gamma_3 \leqq 1$, for $0 < x < \gamma_3$ we have

$$|h(x)| = (1 - x)x(x + \gamma_3)(x + \gamma_4) \cdots (x + \gamma_\nu)$$

$$\geqq (1 - x)x(x + \gamma_3)(-x + \gamma_4) \cdots (-x + \gamma_\nu)$$

(equality only for $\nu = 3$).

From $0 < x < \gamma_3 \leqq 1$ it is easy to verify that

$$(1 - x)(x + \gamma_3) \geqq (1 + x)(-x + \gamma_3)$$

(equality only for $\gamma_3 = 1$). Hence

$$|h(x)| \geqq (1 + x)x(-x + \gamma_3)(-x + \gamma_4) \cdots (-x + \gamma_\nu) = |h(-x)|$$

$$(0 < x < \gamma_3),$$

which establishes lemma 1.

By the argument it is immediately clear that equality holds only for $\nu = 3$ and $\gamma_3 = 1$.

PROOF OF LEMMA 2. We have to prove that if

$$\frac{1}{\gamma_3} + \frac{1}{\gamma_4} + \cdots + \frac{1}{\gamma_{\nu-1}} + \frac{1}{\gamma_\nu} \leqq 1, \tag{4}$$

then

$$\int_{-\gamma_3}^{1} h(x)\,dx \geqq 0.$$

By (4) $\gamma_3 \geqq 1$; thus it will be sufficient to prove that

$$|h(x)| \leqq |h(-x)|. \qquad (0 < x < 1).$$

For $\nu = 3$ we have

$$h(x) = (x-1)x(x+\gamma_3) = (x-1)x(x+1)\frac{x+\gamma_3}{x+1}$$

$$= (x-1)x(x+1)\left(1+\frac{\gamma_3-1}{x+1}\right).$$

If $\gamma_3 = 1$ then $|h(x)| \equiv |h(-x)|$ hence $\int_{-1}^{+1} h(x)\,dx = 0$. If $\gamma_3 > 1$ then

$$1+\frac{\gamma_3-1}{-x+1} > 1+\frac{\gamma_3-1}{x+1} \qquad (0 < x < 1),$$

hence $|h(x)| < |h(-x)|$ $(0 < x < 1)$.

Thus the theorem is true for $\nu = 3$ and we shall prove that if it holds for $\nu - 1$ it also holds for $\nu$ $(\nu \geqq 4)$.

Let us consider the number $\gamma$ for which

$$\frac{1}{\gamma} = \frac{1}{\gamma_{\nu-1}} + \frac{1}{\gamma_\nu}. \tag{5}$$

By (4)

$$\frac{1}{\gamma_3} + \frac{1}{\gamma_4} + \cdots + \frac{1}{\gamma_{\nu-2}} + \frac{1}{\gamma} \leqq 1 \tag{6}$$

and thus

$$1 < \gamma < \gamma_{\nu-1} \leqq \gamma_\nu. \tag{7}$$

In the polynomial of degree $\nu - 1$

$$h^*(x) = h(x)\frac{x+\gamma}{(x+\gamma_{\nu-1})(x+\gamma_\nu)}$$

the coefficient of $x^{\nu-1}$ equals 1, each root is real and by (6) they satisfy (4), hence according to the hypothesis

$$|h^*(x)| \leqq |h^*(-x)|. \qquad (0 < x < 1).$$

By (5) and (7) we easily verify

$$\frac{x+\gamma}{(x+\gamma_{\nu-1})(x+\gamma_\nu)} > \frac{-x+\gamma}{(-x+\gamma_{\nu-1})(-x+\gamma_\nu)} \qquad (0 < x < 1),$$

hence

$$|h(x)| = |h^*(x)| \frac{(x+\gamma_{\nu-1})(x+\gamma_\nu)}{x+\gamma}$$

$$< |h^*(-x)| \frac{(-x+\gamma_{\nu-1})(-x+\gamma_\nu)}{-x+\gamma} = |h(-x)|. \quad (0<x<1),$$

which proves lemma 2.

## 4

Applying the notations of 2 theorem II may be written

$$\int_{a_k}^{a_{k-1}} g(x)\,dx \geqq \frac{2}{3}\left(\frac{a_{k-1}-a_k}{2}\, t_{k-1}\right).$$

If $g'(a_k)$ or $g'(a_{k-1})$ vanishes, $t_{k-1} = 0$ and the theorem becomes trivial, hence we suppose $g'(a_k)g'(a_{k-1}) \neq 0$.

In this case, according to 2

$$t_{k-1} = \frac{a_{k-1}-a_k}{2} \frac{2}{\frac{1}{|g'(a_{k-1})|} + \frac{1}{|g'(a_k)|}} \leqq \frac{a_{k-1}-a_k}{2} (|g'(a_{k-1})|\,|g'(a_k)|)^{\frac{1}{2}} = s_{k-1}.$$

Now we prove that

$$\int_{a_k}^{a_{k-1}} g(x)\,dx \geqq \frac{2}{3}\left(\frac{a_{k-1}-a_k}{2}\, s_{k-1}\right) = \frac{2}{3}\left[\left(\frac{a_{k-1}-a_k}{2}\right)^2 (|g'(a_{k-1})|\,|g'(a_k)|)^{\frac{1}{2}}\right].$$

For $n = 2$ we have equality i.e. our statement holds for $n = 2$. We now suppose that it holds for numbers less than $n$ $(n > 2)$ and prove that it also holds for $n$.

a/ If $2 < k < n$ then $a_{k-1}$ and $a_k$ are at least double roots of the polynomial

$$h(x) = \frac{g(x)}{(x-a_1)(x-a_n)} (x-a_{k-1})(x-a_k)$$

the degree of which is $n$, hence

$$h'(a_{k-1}) = h'(a_k) = 0. \tag{8}$$

On the other hand it is easy to see that

$$0 < h(x) < g(x). \qquad (a_k < x < a_{k-1}). \tag{9}$$

In the polynomials $h(x)$ and $g(x)$, $x^n$ has the same coefficient, hence the degree of the polynomial

$$g_1(x) = g(x) - h(x) (\not\equiv 0)$$

does not exceed $n-1$.

The values $a_2, a_3, \cdots, a_{n-1}$ are roots of $g(x)$ as well as of $h(x)$ thus they are at the same time roots of $g_1(x)$ hence, its coefficients being all real, all roots of $g_1(x)$ must be real too.

By (9), throughout $(a_k, a_{k-1})$ $g_1(x) > 0$ thus $g_1(x)$ satisfies the conditions of theorem II hence according to the hypothesis

$$\int_{a_k}^{a_{k-1}} g_1(x)\,dx \geqq \frac{2}{3}\left[\left(\frac{a_{k-1}-a_k}{2}\right)^2 (|g_1'(a_{k-1})|\,|g_1'(a_k)|)^{\frac{1}{2}}\right].$$

But by (8)

$$g_1'(a_{k-1}) = g'(a_{k-1}), \qquad g_1'(a_k) = g'(a_k),$$

hence, as by (9) $\int_{a_k}^{a_{k-1}} h(x)\,dx > 0$, we have

$$\int_{a_k}^{a_{k-1}} g(x)\,dx = \int_{a_k}^{a_{k-1}} g_1(x)\,dx + \int_{a_k}^{a_{k-1}} h(x)\,dx > \int_{a_k}^{a_{k-1}} g_1(x)\,dx$$

$$\geqq \frac{2}{3}\left[\left(\frac{a_{k-1}-a_k}{2}\right)^2 (|g'(a_{k-1})|\,|g'(a_k)|)^{\frac{1}{2}}\right] = \frac{2}{3}\left[\frac{a_{k-1}-a_k}{2}\,s_{k-1}\right].$$

b/ Of the cases $k = 2$ and $k = n$ it will be sufficient to deal with one of them for this one applied to the polynomial $g(-x)$ settles the other. Then let $k = 2$.

Without any loss of generality we may assume $a_1 = 1$, $a_2 = -1$. In order to satisfy $g(x) > 0$ throughout $(a_2, a_1)$ we must suppose $A$ to be negative. Let $A = -1$ and denote $\alpha_i = -a_i$ $(i = 3, 4, \cdots, n)$. Then

$$g(x) = -(x-1)(x+1)(x+\alpha_3)\cdots(x+\alpha_n),$$

$$1 \leqq \alpha_3 \leqq \alpha_4 \leqq \cdots \leqq \alpha_n$$

and

$$\frac{a_{k-1}-a_k}{2}\,s_k = (|g'(1)|\,|g'(-1)|)^{\frac{1}{2}}.$$

But as, by the hypothesis, $g'(a_1)g'(a_2) = g'(1)g'(-1) \neq 0$ we have

$$1 < \alpha_3 \leqq \alpha_4 \leqq \cdots \leqq \alpha_n. \tag{10}$$

Now consider the polynomial of degree $n-1$

$$g_1(x) = \lambda\,\frac{g(x)}{x+\alpha_n} = -\lambda(x-1)(x+1)(x+\alpha_3)\cdots(x+\alpha_{n-1}) \qquad (\lambda > 0).$$

$g_1(x)$ is positive throughout $(-1, +1)$ and all its roots are real.

Now we choose $\lambda$ so that

$$(|g'(+1)|\,|g'(-1)|)^{\frac{1}{2}} = (|g_1'(+1)|\,|g_1'(-1)|)^{\frac{1}{2}}. \tag{11}$$

Now

$$g'(+1) = -(1+1)(1+\alpha_3)\cdots(1+\alpha_{n-1})(1+\alpha_n),$$

$$g_1'(+1) = -\lambda(1+1)(1+\alpha_3)\cdots(1+\alpha_{n-1}).$$

Hence

$$|g_1'(+1)| = \lambda \frac{|g'(+1)|}{\alpha_n + 1}.$$

Similarly

$$|g_1'(-1)| = \lambda \frac{|g'(-1)|}{\alpha_n - 1},$$

hence

$$|g_1'(+1)|\,|g_1'(-1)| = \frac{\lambda^2}{\alpha_n^2 - 1}\,|g'(+1)|\,|g'(-1)|.$$

(11) will be satisfied if ($\alpha_n > 1$!) $\lambda^2 = \alpha_n^2 - 1 (> 0)$ i.e. if

$$\lambda = +(\alpha_n^2 - 1)^{\frac{1}{2}}.$$

In this case

$$\alpha_n - 1 < \lambda < \alpha_n. \tag{12}$$

Now form the polynomial $h(x) = g_1(x) - g(x)$. Its degree is $n$, its $n - 1$ roots: $+1, -1, -\alpha_3, -\alpha_4, \cdots, -\alpha_{n-1}$ and consequently also the $n^{\text{th}}$ one are all real. We prove that the $n^{\text{th}}$ root must lie in $(-1, 0)$.

By (12)

$$h(0) = g_1(0) - g(0) = \lambda \frac{g(0)}{\alpha_n} - g(0) < 0 \tag{13}$$

and, as $g'(-1) > 0$,

$$h'(-1) = g_1'(-1) - g'(-1) = \frac{\lambda}{\alpha_n - 1} g'(-1) - g'(-1)$$

$$= g'(-1)\left(\frac{\lambda}{\alpha_n - 1} - 1\right) > 0.$$

By this and by $h(-1) = 0$, it follows that somewhere in $(-1, 0)$ $h(x)$ must vanish. Denote this root by $-\alpha$ $(0 < \alpha < 1)$.

$h(x)$ satisfies the requirements of lemma 1 as 1 and $-\alpha$ are simple roots of $h(x)$, $1 - (-\alpha) > (-\alpha) - (-1)$ and as, by (13), throughout $(-1, -\alpha)$ $h(x) > 0$ whereas throughout $(-\alpha, 1)$ $h(x) < 0$. Hence by lemma 1.

$$\int_{-1}^{+1} h(x)\,dx < 0.$$

Consequently

$$\int_{-1}^{+1} g(x)\,dx = \int_{-1}^{+1} g_1(x)\,dx - \int_{-1}^{+1} h(x)\,dx > \int_{-1}^{+1} g_1(x)\,dx.$$

But $g_1(x)$ is of degree $n-1$. Thus by the hypothesis

$$\int_{-1}^{+1} g_1(x)\,dx \geqq \tfrac{2}{3}(|g_1'(+1)|\,|g_1'(-1)|)^{\frac{1}{2}},$$

which with (11) gives

$$\int_{-1}^{+1} g(x)\,dx > \tfrac{2}{3}(|g'(+1)|\,|g'(-1)|)^{\frac{1}{2}},$$

which proves theorem II.

## 5

By applying the notations introduced in 2, we write theorem III in the form

$$\int_{a_k}^{a_{k-1}} g(x)\,dx \leqq \tfrac{2}{3}(a_{k-1}-a_k)g(b_{k-1}).$$

We prove it by induction. Theorem III holds for $n=2$ (equality). We shall prove that if it is true for numbers less than $n$ ($n>2$) then it also holds for $n$.

a/ If $2<k<n$ then $a_k$ and $a_{k-1}$ are at least simple roots of the polynomial of degree $n$

$$h(x)=\frac{g(x)}{(x-a_1)(x-a_n)}(x-b_{k-1})^2$$

whereas $b_{k-1}$ is exactly a double root. Thus $h(b_{k-1})=h'(b_{k-1})=0$. In the interior of the intervals $(a_k, a_{k-1})$, with the exception of $b_{k-1}$, $h(x)$ is less than 0.

The coefficient of $x^n$ in $h(x)$ and in $g(x)$ is the same, thus the degree of the polynomial $g_1(x)=g(x)-h(x)$ does not exceed $n-1$. All roots of $g_1(x)$ are real, for it vanishes at $a_2, a_3, \cdots, a_{k-1}, a_k, \cdots a_{n-1}$ and thus the eventually resulting $(n-1)^{\text{th}}$ root cannot be complex. Hence, as $g_1'(b_{k-1})=g'(b_{k-1})-h'(b_{k-1})=0$ we have by hypothesis

$$\int_{a_k}^{a_{k-1}} g_1(x)\,dx \leqq \tfrac{2}{3}(a_{k-1}-a_k)g_1(b_{k-1}).$$

But as

$$g_1(b_{k-1})=g(b_{k-1})-h(b_{k-1})=g(b_{k-1})$$

and since throughout $(a_k, a_{k-1})$ (with the exception of $x=b_{k-1}$, when equality holds) $g_1(x)>g(x)$ we may write

$$\int_{a_k}^{a_{k-1}} g_1(x)\,dx > \int_{a_k}^{a_{k-1}} g(x)\,dx,$$

hence

$$\int_{a_k}^{a_{k-1}} g(x)\,dx < \tfrac{2}{3}(a_{k-1}-a_k)g(b_{k-1}).$$

b/ Just as in 4 we have to consider only one of the cases $k=2$ and $k=n$.

Let $k = 2$. Consider the polynomial of degree $n - 1$

$$g_1(x) = \lambda \frac{g(x)}{x - a_n}. \qquad (\lambda > 0).$$

We choose $\lambda$ such as to make the maximal value of $g_1(x)$ in $(a_2, a_1)$ (positive in this interval as well as that of $g(x)$) equal to that of $g(x)$. Such a $\lambda$ exists. Hence, denoting the root of $g_1'(x)$ lying in $(a_2, a_1)$ by $b$, we have

$$g_1(b) = g(b_1). \tag{14}$$

From the equations

$$\frac{g'(b_1)}{g(b_1)} = 0 \quad \text{and} \quad \frac{g_1'(b)}{g_1(b)} = 0$$

we obtain

$$\frac{1}{b_1 - a_2} + \frac{1}{b_1 - a_3} + \cdots + \frac{1}{b_1 - a_{n-1}} + \frac{1}{b_1 - a_n} = \frac{1}{a_1 - b_1}$$

and

$$\frac{1}{b - a_2} + \frac{1}{b - a_3} + \cdots + \frac{1}{b - a_{n-1}} = \frac{1}{a_1 - b}. \tag{15}$$

By which

$$b < b_1.$$

The polynomial $h(x) = g_1(x) - g(x)$ is of degree $n$. Its $n - 1$ roots are $a_1, a_2, a_3, \cdots, a_{n-1}$. Furthermore, it must vanish in the interval $(b, b_1)$ too, since by (14)

$$h(b) = g_1(b) - g(b) > 0 \quad \text{and} \quad h(b_1) = g_1(b_1) - g(b_1) < 0.$$

Denote the root of $h(x)$ lying in $(b, b_1)$ by $a$. By (15)

$$\frac{1}{a - a_2} + \frac{1}{a - a_3} + \cdots + \frac{1}{a - a_{n-1}} < \frac{1}{a_1 - a},$$

hence, $a_1$ and $a$ being simple roots, $h(x)$ satisfies all the conditions of lemma 2. Hence

$$\int_{a_2}^{a_1} h(x)\,dx > 0.$$

From this we obtain

$$\int_{a_2}^{a_1} g(x)\,dx = \int_{a_2}^{a_1} g_1(x)\,dx - \int_{a_2}^{a_1} h(x)\,dx < \int_{a_2}^{a_1} g_1(x)\,dx.$$

But according to the hypothesis, the degree of $g_1(x)$ being less than $n$,

$$\int_{a_2}^{a_1} g_1(x)\,dx \leqq \tfrac{2}{3}(a_1 - a_2)g_1(b),$$

hence by (14) we have

$$\int_{a_2}^{a_1} g(x)\,dx < \tfrac{2}{3}(a_1 - a_2)g(b_1),$$

and thus theorem III is completely proved.

INSTITUTE FOR ADVANCED STUDY, PRINCETON, N. J., AND BUDAPEST, HUNGARY.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# TRANSFORMATIONEN VON ALGEBRAISCHEM TYP

BY HERMANN KOBER

(Received August 4, 1938)

1. Sei $\mathfrak{L}_2(a, b)$, $-\infty \leqq a < b \leqq \infty$, der Hilbertsche Raum, der aus allen komplexwertigen Funktionen von $L^2(a, b)$ besteht, mit dem inneren Produkt

$$(f, g) = \int_a^b f(x)\bar{g}(x)\,dx,$$

$\mathfrak{H}$ irgendein Hilbertscher Raum mit entsprechend festgelegter Metrik, sei $\|f\| = (f, f)^{\frac{1}{2}} \geqq 0$; $f_n \sim f$ bedeute $\lim \|f - f_n\| = 0$ für $n \to \infty$. Die Hankelsche[1] Transformation $g = Tf$,

$$(1) \qquad g(x) = \underset{n\to\infty}{\text{l.i.m.}} \int_0^n J_\alpha(tx)\sqrt{(tx)}f(t)\,dt, \qquad \Re(\alpha) > -1, f \in \mathfrak{L}_2(0, \infty)$$

ist involutorisch, es ist also $T^2f = f$, und aus dieser Beziehung algebraischer Art lassen sich wesentliche Eigenschaften von $T$ folgern. Ähnlich ist es z.B. bei der Fourier-Transformation $g = Sf$,

$$(2) \qquad g(x) = \underset{\substack{n\to\infty \\ q\to\infty}}{\text{l.i.m.}} \int_{-q}^{n} e^{itx}f(t)\,dt, \qquad f \in \mathfrak{L}_2(-\infty, \infty),$$

für welche $f(-x) = Sg(x)$, also $S^4f - f = 0$ ist. So gelangt man zur Betrachtung folgender Klasse von Transformationen $T$:

(A) *Der Bereich ("domain") sei $\mathfrak{D}_T$, $T$ sei linear, habe nur endlich viele verschiedene Eigenwerte $l_q$ ($q = 0, 1, \cdots, k-1$; $k \geqq 1$), und die Eigenfunktionen sollen die, ersichtlich lineare, Mannigfaltigkeit $\mathfrak{D}_T$ in $\mathfrak{H}$ bestimmen.*[2]

Ersichtlich müssen Integraloperatoren, durch welche Transformationen dieser Art sich darstellen lassen, singulär sein. Man kommt weiter zu folgender Definition und zunächst zu folgenden Sätzen:

(B) DEFINITION: *Sei $g = Sf$ eine lineare Transformation in $\mathfrak{H}$ von folgenden Eigenschaften:*

---

[1] E. C. Titchmarsh, Proc. Cambridge Phil. Soc. 21 (1923), 463-73, $\alpha \geqq -\frac{1}{2}$, und J. of London Math. Soc. 1 (1926), 195-6. Ausdehnung für alle $\alpha$ ausser für $\Re\alpha = -1, -3, -5, \cdots$. Verfasser, Quart. J. of Math. (Oxford) 8 (1937), 186-99. Ferner Verf. II und III, Proc. London Math. Soc. (2) 44 (1938), 453-65, u. 45 (1939) 229-42. Es ist l.i.m. Abkürzung für limes im Quadratmittel. In (2) hat itæ aus Bequemlichkeitsgründen nicht das übliche negative Vorzeichen.

[2] M. H. Stone, *Linear Transformations in Hilbert Space*, New York 1932, Def. 1.4, 2.1, Theor. 2.3.—Falls Null Eigenwert ist, sind die zugehörigen Eigenfunktionen die Lösungen von $Tf = 0$.

(i) *Für jede Funktion $f$ aus $\mathfrak{D}_S$, dem nicht leeren Bereiche ("domain") von $S$, gehört auch $g$ zu $\mathfrak{D}_S$.*
(ii) *Es gibt ein Polynom* $P_m(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x^1 + a_0x^0$ mit lauter einfachen Nullstellen, der Art, dass $P_m(Sf)$ für jedes $f \in \mathfrak{D}_S$ Null ist,

$$P_m(Sf) = S^m f + a_{m-1}S^{m-1}f + \cdots + a_1 Sf + a_0 S^0 f = 0, \qquad f \in \mathfrak{D}_S;$$

*dann ist $S$ eine "Transformation von algebraischem Typ." Der "Grad" von $S$ sei der eines der Bedingung genügenden Polynoms $P_m$ von kleinstmöglichem Grade.*

Bedeute $S^0$ die identische Transformation $I$, also $S^0 f = If = f$.

SATZ I. *Jede Transformation der Art* (A) *ist eine der Art* (B) *vom Grade $k$ und umgekehrt.*

SATZ II. *Jede Funktion aus $\mathfrak{D}_S$* (Def. B) *ist eindeutig als Summe von höchstens $k$ zu verschiedenen Eigenwerten gehörigen Eigenfunktionen darstellbar, andere Funktionen nicht.*

Dann werden hier solche Transformationen behandelt, die ausserdem abgeschlossen oder beschränkt (stetig) oder unitär sind u.s.w.[3] (Abschn. 3), Fragen der Umkehrbarkeit und des Spektrums (Abschn. 4) sowie abgeschlossene Systeme im Raume der einem festen Eigenwerte entsprechenden Eigenfunktionen (Abschn. 5). Zum Schlusse werden Beispiele gegeben, darunter sehr einfache Transformationen, die man als $k$. Wurzel ($k = 2, 3, \cdots$) aus der Fourier- bezw. Hankel-Transformation auffassen kann, und die bisher nicht bekannt sind. Die hier sich ergebenden Sätze über abgeschlossene Systeme in einem Raume von Eigenfunktionen scheinen auch im Falle der gewöhnlichen Hankel-Transformation neu zu sein. Die Konstruktion aller in $\mathfrak{H}$ vorhandenen Transformationen von algebraischem Typ wird durch Satz VII (Abschn. 7) ermöglicht.

**2.** BEWEIS DER SÄTZE I UND II. Sei $S$ vom algebraischen Typ, seien $l_0, l_1, \cdots, l_{m-1}$ die, sämtlich verschiedenen, Nullstellen des Polynoms $P_m(x)$ (Def. B), dann ist wegen $P_m(Sf) = 0$ und der Linearität von $S$ bei beliebiger Reihenfolge der Faktoren, mit Rücksicht auf $S^n I = IS^n$ u.s.w.,

$$(2.0)\quad P_m(Sf) = \left\{\prod_{q=0}^{m-1}(S - l_q I)\right\} f = (S - l_{m-1}I)(S - l_{m-2}I)\cdots(S - l_0 I)f = 0.$$

Mindestens eine der Nullstellen $l_q$ muss ein Eigenwert sein: seien etwa $l_1, l_2, \cdots l_{m-1}$ es nicht, so hat keine der Gleichungen $(S - l_q I)\psi = 0$, $(q = 1, 2, \cdots, m-1)$, eine von Null verschiedene Lösung $\psi \in \mathfrak{D}_S$. Aus (2, 0) würde daher schrittweise folgen, dass jede der folgenden Transformationen, deren Bereiche gleich $\mathfrak{D}_S$ sind,

$$\left\{\prod_{q=0}^{m-2}(S - l_q I)\right\} f; \left\{\prod_{q=0}^{m-3}(S - l_q I)\right\} f; \cdots \left\{\prod_{q=0}^{0}(S - l_q I)\right\} f = Sf - l_0 f$$

[3] M. H. Stone, Def. 2.5, 2.4, 2.18, 2.11, Theor. 2.21. Spektrum: Chapter IV, §2 u.s.w.

den Wert Null hat, dass daher $Sf = l_0 f$, $l_0$ sicher ein Eigenwert ist. Seien also $l_0, l_1, \cdots l_{k-1}$, $1 \leqq k \leqq m$, genau diejenigen $l_q$, welche Eigenwerte sind, $P_k(x) = \prod(x - l_q)$, $(q = 0, 1, \cdots, k-1)$, $P_k(x)$ somit ein Teiler von $P_m(x)$ und $P_k(Sf)$ Null für alle $f$ aus $\mathfrak{D}_S$, sei $\mathfrak{R}_q$ die, der Linearität von $S$ wegen sicher lineare, Menge der zu $l_q$ gehörigen Eigenfunktionen $\varphi_q$ mit Hinzunahme des Elementes Null. Zwei Räume $\mathfrak{R}_n$ und $\mathfrak{R}_q$, $n \neq q$, haben nur das Element Null gemeinsam; denn aus $S\varphi = l_n\varphi$ und $S\varphi = l_q\varphi$ folgt $(l_n - l_q)\varphi = 0$, also $\varphi = 0$.

HILFSSATZ Ia. *Seien $S$, $P_k(x)$, $\mathfrak{R}_q$ wie oben definiert, $f$ aus $\mathfrak{D}_S$ beliebig gegeben,*

$$(2.1)\quad Q_q(x) = c_q P_k(x)/(x - l_q);\ c_q^{-1} = \left(\frac{d}{dx} P_k(x)\right)_{x=l_q};\quad q = 0, 1, \cdots, k-1.$$

$$(2.2)\quad \psi_q = Q_q(Sf) = c_q\{\prod(S - l_n I)\}f, \qquad n = 0, 1, \cdots, k-1,\ n \neq q.$$

*($\alpha$) Dann ist $\psi_q$ eine zum Eigenwerte $l_q$ gehörige Eigenfunktion oder Null.*
*($\beta$) $f = \psi_0 + \psi_1 + \cdots + \psi_{k-1}$, $\psi_q \in \mathfrak{R}_q$.*
*($\gamma$) Die Darstellung von $f$ in der Form ($\beta$) ist eindeutig.*
*($\delta$) Jede Funktion von der Form $\varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} (\varphi_q \in \mathfrak{R}_q)$ gehört zu $\mathfrak{D}_S$.*

BEWEIS VON Ia. Es ist mit Rücksicht auf (2.2)

$$S\psi_q = (S - l_q I)\psi_q + l_q\psi_q = c_q\left\{\prod_{n=0}^{k-1}(S - l_n I)\right\}f + l_q\psi_q,$$

$$(\alpha)\qquad S\psi_q = c_q P_k(Sf) + l_q\psi_q = l_q\psi_q,$$

also $\psi_q$ aus $\mathfrak{R}_q$. Identisch in $x$ ist bekanntlich $\sum Q_q(x) = x^0$, $(q = 0, 1, \cdots, k-1)$, daher folgt durch Vergleichung der Koeffizienten

$$f = S^0 f = Q_0(Sf) + Q_1(Sf) + \cdots + Q_{k-1}(Sf),$$

also ($\beta$). Umgekehrt sind durch $f$ aus ($\beta$) die Funktionen $\psi_q$, da $\psi_q \in \mathfrak{R}_q$ gefordert wird, eindeutig bestimmt; denn aus ($\beta$) folgt dann

$$Q_q(Sf) = Q_q(S\psi_0) + Q_q(S\psi_1) + \cdots + Q_q(S\psi_{k-1}) = \psi_q,$$

weil

$$(2.3)\qquad Q_q(S\psi_n) = \psi_q \text{ für } n = q, \qquad Q_q(S\psi_n) = 0 \text{ für } n \neq q$$

ist; z.B. ist wegen $(S - l_q I)\psi_q = 0$ bezw. $(S - l_n I)\psi_q = (l_q - l_n)\psi_q$

$$Q_0(S\psi_1) = c_0\left\{\prod_{n=1}^{k-1}(S - l_n I)\right\}\psi_1 = c_0\left\{\prod_{n=2}^{k-1}(S - l_n I)\right\}(S - l_1 I)\,\psi_1 = 0,$$

$$Q_0(S\psi_0) = c_0\left\{\prod_{n=1}^{k-1}(S - l_n I)\right\}\psi_0$$

$$= c_0\left\{\prod_{n=2}^{k-1}(S - l_n I)\right\}(l_0 - l_1)\psi_0 = \cdots = c_0\psi_0\prod_{n=1}^{k-1}(l_0 - l_n) = \psi_0.$$

Die Behauptung ($\delta$) ist wegen $\mathfrak{R}_q \subset \mathfrak{D}_S$ einleuchtend.
Die Transformation $Q_q(Sf)$ kann man als *Projektion* von $\mathfrak{D}_S$ auf $\mathfrak{R}_q$ auffassen.

HILFSSATZ Ib. *Die Transformation $S$ des Hilfssatzes Ia hat ausser $l_0, l_1, \cdots, l_{k-1}$ keine weiteren Eigenwerte.*

Wäre nämlich $l$ von allen $l_q$ verschieden und Eigenwert, so wäre $S\varphi = l\varphi$,

$$P_k(S\varphi) = \left\{\prod_{q=0}^{k-1}(S - l_qI)\right\}\varphi = \left\{\prod_{q=1}^{k-1}(S - l_qI)\right\}(l - l_0)\,\varphi = \cdots = \varphi\prod_{q=0}^{k-1}(l - l_q),$$

also $\varphi = 0$ wegen $P_k(S\varphi) = 0$ und $\prod(l - l_q) \neq 0$, ein Widerspruch.

Aus Hilfssatz Ib, der Verschiedenheit der Eigenwerte $l_0, l_1, \cdots, l_{k-1}$ und aus Ia, ($\beta$) und ($\delta$) folgt die Identität der Transformation $S$ mit einer von der Art (A), aus ($\beta$), ($\gamma$) und ($\delta$) dann Satz II.

Ist umgekehrt $T$ von der Art (A), $\psi_q \in \mathfrak{R}_q (q = 0, 1, \cdots, k-1)$, also $T\psi_q = l_q\psi_q$, so ist $l_q$ endlich, ferner jede Funktion $f$ aus $\mathfrak{D}_T$ als lineare ganze Verbindung endlich vieler Eigenfunktionen darstellbar, weil die Eigenfunktionen die lineare Mannigfaltigkeit $\mathfrak{D}_T$ bestimmen sollen, $f$ also sicher schliesslich in die Form ($\beta$) zu bringen. Durch mehrfache Anwendung der linearen Transformation $T$ folgt

$$T^n f = l_0^n\psi_0 + l_1^n\psi_1 + \cdots + l_{k-1}^n\psi_{k-1}, \qquad n = 0, 1, \cdots, k. \tag{2.4}$$

Aus $\psi_q \in \mathfrak{D}_T$ und der Linearität von $T$ folgt $T^n f \in \mathfrak{D}_T$ $(n = 0, 1, \cdots, k)$. Durch Elimination der Funktionen $\psi_0, \psi_1, \cdots, \psi_{k-1}$ aus den $k+1$ Gleichungen (2.4) folgt nach bekannten Sätzen der Algebra

$$T^k f + a_{k-1}T^{k-1}f + \cdots + a_1T^1 f + a_0T^0 f = 0,$$

wenn $P_k(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$ das Polynom mit den, sämtlich verschiedenen, Nullstellen $l_0, l_1, \cdots, l_{k-1}$ vom Grade $k$ und mit $a_k = 1$ ist. Also ist $T$ von algebraischem Typ. Der Grad von $T$ ist $k$; wäre $P_n(Tf)$ Null für alle $f$ aus $\mathfrak{D}_T$ und wäre $n < k$, so hätte $T$ nach Ib nur $n$ Eigenwerte, gegen die Voraussetzung. Somit sind die Sätze I und II bewiesen.—Aus Ia ($\gamma$) folgt

ZUSATZ Ic. *Die linearen Mannigfaltigkeiten $\mathfrak{R}_0, \mathfrak{R}_1, \cdots, \mathfrak{R}_{k-1}$ sind "linear unabhängig," d.h. eine Funktion $\varphi_0 + \varphi_1 + \cdots + \varphi_{k-1}$ mit $\varphi_q \in \mathfrak{R}_q$ kann nur für $\varphi_1 = \varphi_2 = \varphi_3 = \cdots = 0$ verschwinden.*

**3.** SATZ III. *Wenn die Transformation $g = Sf$ in $\mathfrak{H}$ von algebraischem Typ mit dem Grade $k$ und*

($\alpha$) *abgeschlossen ist, sind $\mathfrak{R}_0, \mathfrak{R}_1, \cdots, \mathfrak{R}_{k-1}$ abgeschlossene lineare Mannigfaltigkeiten; mindestens ein $\mathfrak{R}_q$ ist dann ein Hilbertscher Raum, wenn nicht $\mathfrak{D}_S$ nur endlich viele linear unabhängige Elemente enthält.*

($\beta$) *beschränkt (stetig) ist, dann und nur dann gibt es eine feste positive Zahl $A$ der Art, dass für $\varphi_0 \in \mathfrak{R}_0$, $\varphi_1 \in \mathfrak{R}_1, \cdots$ stets $\|\varphi_q\| \leqq A\,\|\varphi_0 + \varphi_1 + \cdots \varphi_{k-1}\|$ ist, $q = 0, 1, 2, \cdots k-1$. Der bestmögliche Wert von $A$ ist dann und nur dann Eins, wenn je zwei Räume $\mathfrak{R}_n$ und $\mathfrak{R}_q$ zueinander orthogonal sind.*

($\gamma$) *unitär ist, dann und nur dann sind alle Eigenwerte vom Absolutwert Eins und je zwei Räume $\mathfrak{R}_n, \mathfrak{R}_q$ zueinander orthogonal und $\mathfrak{D}_S = \mathfrak{H}$.*

(δ) *selbstadjungiert ist, dann und nur dann sind alle Eigenwerte reell und je zwei Räume* $\mathfrak{R}_n$, $\mathfrak{R}_q$ *zueinander orthogonal und* $\mathfrak{D}_S = \mathfrak{H}$.

BEWEIS. (α) Sei $S$ abgeschlossen, also für $f_n \sim f$, $g_n \sim g$ und $Sf_n = g_n$ dann $Sf = g$. Sei $\{\varphi_{q,n}\}$, $n = 0, 1, 2, \cdots$, irgendeine Funktionenfolge aus $\mathfrak{R}_q$, die gegen eine Grenzfunktion $\psi$ im Quadratmittel konvergiere, also $S\varphi_{q,n} = l_q\varphi_{q,n}$, $\varphi_{q,n} \sim \psi$, folglich $S\psi = l_q\psi$, d.h. $\psi \in \mathfrak{R}_q$, $\mathfrak{R}_q$ ist abgeschlossen. Falls jedes $\mathfrak{R}_q$ nur endlich viele linear unabhängige Elemente enthält, gilt wegen Satz II das Gleiche für $\mathfrak{D}_S$ (cf. Stone, Theor. 1.19).

(β) Sei $S$ stetig (beschränkt), also $\| Sf \| \leqq B \| f \|$ für alle $f$ aus $\mathfrak{D}_S$; ersichtlich ist dann jede Transformation $Q_q(Sf)$ (s. Ia, 2.1, 2.2) beschränkt, $\| Q_q(Sf) \| \leqq A \| f \|$, $q = 0, 1, \cdots, k-1$. Sei nun $\varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} = f$, $\varphi_q \in \mathfrak{R}_q (q = 0, 1, \cdots)$, so ist $\varphi_q = Q_q(Sf)$, also $\| \varphi_q \| \leqq A \| f \| = A \| \varphi_1 + \varphi_2 + \cdots + \varphi_{k-1} \|$.

Sei umgekehrt $f \in \mathfrak{D}_S$ beliebig gegeben, $f = \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1}$ (Satz II), daher $Sf = l_0\varphi_0 + l_1\varphi_1 + \cdots l_{k-1}\varphi_{k-1}$, $\varphi_q \in \mathfrak{R}_q$. Aus $\| \varphi_q \| \leqq A \| \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} \|$ folgt $\| Sf \| \leqq \max | l_q | \{ \| \varphi_0 \| + \| \varphi_1 \| + \cdots \} \leqq \max | l_q | kA \| \varphi_0 + \varphi_1 + \cdots \| = \max | l_q | kA \| f \|$, also ist $Sf$ beschränkt. Sind z.B. je zwei Räume $\mathfrak{R}_n$, $\mathfrak{R}_q$ zueinander orthogonal, so ist $\| \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} \|^2 = \| \varphi_0 \|^2 + \| \varphi_1 \|^2 + \cdots + \| \varphi_{k-1} \|^2 \geqq \| \varphi_q \|^2$, $A = 1$, $S$ stetig; der Beweis der Umkehrung soll nicht ausgeführt werden.

(γ) Sei $S$ unitär in $\mathfrak{H}$,[4] und daher sei $\mathfrak{D}_S = \mathfrak{H}$, ferner für alle $f_1$ und $f_2$ aus $\mathfrak{H}$ $(Sf_1, Sf_2) = (f_1, f_2)$; so ist für $\varphi_n \in \mathfrak{R}_n$, $\varphi_q \in \mathfrak{R}_q$, $\varphi \neq 0$: $(\varphi_n, \varphi_q) = (S\varphi_n, S\varphi_q) = (l_n\varphi_n, l_q\varphi_q) = l_n\overline{l_q}(\varphi_n, \varphi_q)$. Hieraus folgt für $q = n$, dass $| l_q | = 1$, für $q \neq n$, dass $(\varphi_n, \varphi_q) = 0$, also $\mathfrak{R}_n$ orthogonal zu $\mathfrak{R}_q$ ist. Umgekehrt folgt aus $\mathfrak{D}_S = \mathfrak{H}$, $| l_q | = 1$ und aus $(\varphi_n, \varphi_q) = 0$ für $n \neq q$, dass $S$ unitär ist: Für $f_1 \in \mathfrak{D}_S$, $f_2 \in \mathfrak{D}_S$ ist

$$f_1 = \varphi_{0,1} + \varphi_{1,1} + \cdots + \varphi_{k-1,1}, \qquad f_2 = \varphi_{0,2} + \varphi_{1,2} + \cdots + \varphi_{k-1,2},$$

$$\varphi_{q,1} \in \mathfrak{R}_q, \ \varphi_{q,2} \in \mathfrak{R}_q,$$

$$(Sf_1, Sf_2) = (l_0\varphi_{0,1} + l_1\varphi_{1,1} + \cdots, l_0\varphi_{0,2} + l_1\varphi_{1,2} + \cdots)$$

$$= \sum_{q=0}^{k-1} | l_q |^2 (\varphi_{q,1}, \varphi_{q,2}) = \sum_{q=0}^{k-1} (\varphi_{q,1}, \varphi_{q,2}) = (f_1, f_2).$$

Da nun $\mathfrak{D}_S = \mathfrak{H}$ ist, ist auch der Vorrat ("range") gleich $\mathfrak{H}$ (Satz IV), $S$ unitär.

Der Beweis von III (δ) ergibt sich durch entsprechende Überlegungen.

## 4. Die Fragen der Umkehrbarkeit und des Spektrums beantwortet

Satz IV. *Sei $S$ von algebraischem Typ, $S_l = S - lI$. Wenn $l$ von allen Eigenwerten von $S$ verschieden ist, dann und nur dann ist $S_l$ umkehrbar, dann und nur dann der Vorrat ("range") von $S_l$ gleich dem Bereiche $\mathfrak{D}_S$ von $S$. Die Umkehrung $S_l^{-1}$ ist dann und nur dann beschränkt, wenn $S$ es ist.*

HILFSSATZ IVa. *Wenn in einer Transformation $S$ von algebraischem Typ kein Eigenwert Null ist, dann und nur dann ist $S$ umkehrbar, dann und nur dann der*

[4] C.f. M. H. Stone, Theorem 8.2.

HILFSSATZ IB. *Die Transformation $S$ des Hilfssatzes Ia hat ausser $l_0, l_1, \cdots, l_{k-1}$ keine weiteren Eigenwerte.*

Wäre nämlich $l$ von allen $l_q$ verschieden und Eigenwert, so wäre $S\varphi = l\varphi$,

$$P_k(S\varphi) = \left\{\prod_{q=0}^{k-1}(S - l_qI)\right\}\varphi = \left\{\prod_{q=1}^{k-1}(S - l_qI)\right\}(l - l_0)\,\varphi = \cdots = \varphi\prod_{q=0}^{k-1}(l - l_q),$$

also $\varphi = 0$ wegen $P_k(S\varphi) = 0$ und $\prod(l - l_q) \neq 0$, ein Widerspruch.

Aus Hilfssatz Ib, der Verschiedenheit der Eigenwerte $l_0, l_1, \cdots, l_{k-1}$ und aus Ia, ($\beta$) und ($\delta$) folgt die Identität der Transformation $S$ mit einer von der Art (A), aus ($\beta$), ($\gamma$) und ($\delta$) dann Satz II.

Ist umgekehrt $T$ von der Art (A), $\psi_q \in \mathfrak{R}_q (q = 0, 1, \cdots, k-1)$, also $T\psi_q = l_q\psi_q$, so ist $l_q$ endlich, ferner jede Funktion $f$ aus $\mathfrak{D}_T$ als lineare ganze Verbindung endlich vieler Eigenfunktionen darstellbar, weil die Eigenfunktionen die lineare Mannigfaltigkeit $\mathfrak{D}_T$ bestimmen sollen, $f$ also sicher schliesslich in die Form ($\beta$) zu bringen. Durch mehrfache Anwendung der linearen Transformation $T$ folgt

$$T^n f = l_0^n\psi_0 + l_1^n\psi_1 + \cdots + l_{k-1}^n\psi_{k-1}, \qquad n = 0, 1, \cdots, k. \tag{2.4}$$

Aus $\psi_q \in \mathfrak{D}_T$ und der Linearität von $T$ folgt $T^n f \in \mathfrak{D}_T$ ($n = 0, 1, \cdots, k$). Durch Elimination der Funktionen $\psi_0, \psi_1, \cdots, \psi_{k-1}$ aus den $k+1$ Gleichungen (2.4) folgt nach bekannten Sätzen der Algebra

$$T^k f + a_{k-1}T^{k-1}f + \cdots + a_1T^1 f + a_0T^0 f = 0,$$

wenn $P_k(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$ das Polynom mit den, sämtlich verschiedenen, Nullstellen $l_0, l_1, \cdots, l_{k-1}$ vom Grade $k$ und mit $a_k = 1$ ist. Also ist $T$ von algebraischem Typ. Der Grad von $T$ ist $k$; wäre $P_n(Tf)$ Null für alle $f$ aus $\mathfrak{D}_T$ und wäre $n < k$, so hätte $T$ nach Ib nur $n$ Eigenwerte, gegen die Voraussetzung. Somit sind die Sätze I und II bewiesen.—Aus Ia ($\gamma$) folgt

ZUSATZ IC. *Die linearen Mannigfaltigkeiten $\mathfrak{R}_0, \mathfrak{R}_1, \cdots, \mathfrak{R}_{k-1}$ sind "linear unabhängig," d.h. eine Funktion $\varphi_0 + \varphi_1 + \cdots + \varphi_{k-1}$ mit $\varphi_q \in \mathfrak{R}_q$ kann nur für $\varphi_1 = \varphi_2 = \varphi_3 = \cdots = 0$ verschwinden.*

**3.** SATZ III. *Wenn die Transformation $g = Sf$ in $\mathfrak{H}$ von algebraischem Typ mit dem Grade $k$ und*

($\alpha$) *abgeschlossen ist, sind $\mathfrak{R}_0, \mathfrak{R}_1, \cdots, \mathfrak{R}_{k-1}$ abgeschlossene lineare Mannigfaltigkeiten; mindestens ein $\mathfrak{R}_q$ ist dann ein Hilbertscher Raum, wenn nicht $\mathfrak{D}_S$ nur endlich viele linear unabhängige Elemente enthält.*

($\beta$) *beschränkt (stetig) ist, dann und nur dann gibt es eine feste positive Zahl $A$ der Art, dass für $\varphi_0 \in \mathfrak{R}_0, \varphi_1 \in \mathfrak{R}_1, \cdots$ stets $\|\varphi_q\| \leqq A\,\|\varphi_0 + \varphi_1 + \cdots \varphi_{k-1}\|$ ist, $q = 0, 1, 2, \cdots k-1$. Der bestmögliche Wert von $A$ ist dann und nur dann Eins, wenn je zwei Räume $\mathfrak{R}_n$ und $\mathfrak{R}_q$ zueinander orthogonal sind.*

($\gamma$) *unitär ist, dann und nur dann sind alle Eigenwerte vom Absolutwert Eins und je zwei Räume $\mathfrak{R}_n, \mathfrak{R}_q$ zueinander orthogonal und $\mathfrak{D}_S = \mathfrak{H}$.*

($\delta$) *selbstadjungiert ist, dann und nur dann sind alle Eigenwerte reell und je zwei Räume* $\mathfrak{R}_n$, $\mathfrak{R}_q$ *zueinander orthogonal und* $\mathfrak{D}_S = \mathfrak{H}$.

BEWEIS. ($\alpha$) Sei $S$ abgeschlossen, also für $f_n \sim f$, $g_n \sim g$ und $Sf_n = g_n$ dann $Sf = g$. Sei $\{\varphi_{q,n}\}$, $n = 0, 1, 2, \cdots$, irgendeine Funktionenfolge aus $\mathfrak{R}_q$, die gegen eine Grenzfunktion $\psi$ im Quadratmittel konvergiere, also $S\varphi_{q,n} = l_q\varphi_{q,n}$, $\varphi_{q,n} \sim \psi$, folglich $S\psi = l_q\psi$, d.h. $\psi \in \mathfrak{R}_q$, $\mathfrak{R}_q$ ist abgeschlossen. Falls jedes $\mathfrak{R}_q$ nur endlich viele linear unabhängige Elemente enthält, gilt wegen Satz II das Gleiche für $\mathfrak{D}_S$ (cf. Stone, Theor. 1.19).

($\beta$) Sei $S$ stetig (beschränkt), also $\| Sf \| \leqq B \| f \|$ für alle $f$ aus $\mathfrak{D}_S$; ersichtlich ist dann jede Transformation $Q_q(Sf)$ (s. Ia, 2.1, 2.2) beschränkt, $\| Q_q(Sf) \| \leqq A \| f \|$, $q = 0, 1, \cdots, k-1$. Sei nun $\varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} = f$, $\varphi_q \in \mathfrak{R}_q (q = 0, 1, \cdots)$, so ist $\varphi_q = Q_q(Sf)$, also $\| \varphi_q \| \leqq A \| f \| = A \| \varphi_1 + \varphi_2 + \cdots + \varphi_{k-1} \|$.

Sei umgekehrt $f \in \mathfrak{D}_S$ beliebig gegeben, $f = \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1}$ (Satz II), daher $Sf = l_0\varphi_0 + l_1\varphi_1 + \cdots l_{k-1}\varphi_{k-1}$, $\varphi_q \in \mathfrak{R}_q$. Aus $\| \varphi_q \| \leqq A \| \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} \|$ folgt $\| Sf \| \leqq \max | l_q | \{ \| \varphi_0 \| + \| \varphi_1 \| + \cdots \} \leqq \max | l_q | kA \| \varphi_0 + \varphi_1 + \cdots \| = \max | l_q | kA \| f \|$, also ist $Sf$ beschränkt. Sind z.B. je zwei Räume $\mathfrak{R}_n$, $\mathfrak{R}_q$ zueinander orthogonal, so ist $\| \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1} \|^2 = \| \varphi_0 \|^2 + \| \varphi_1 \|^2 + \cdots + \| \varphi_{k-1} \|^2 \geqq \| \varphi_q \|^2$, $A = 1$, $S$ stetig; der Beweis der Umkehrung soll nicht ausgeführt werden.

($\gamma$) Sei $S$ unitär in $\mathfrak{H}$,[4] und daher sei $\mathfrak{D}_S = \mathfrak{H}$, ferner für alle $f_1$ und $f_2$ aus $\mathfrak{H}$ $(Sf_1, Sf_2) = (f_1, f_2)$; so ist für $\varphi_n \in \mathfrak{R}_n$, $\varphi_q \in \mathfrak{R}_q$, $\varphi \neq 0$: $(\varphi_n, \varphi_q) = (S\varphi_n, S\varphi_q) = (l_n\varphi_n, l_q\varphi_q) = l_n\overline{l_q}(\varphi_n, \varphi_q)$. Hieraus folgt für $q = n$, dass $| l_q | = 1$, für $q \neq n$, dass $(\varphi_n, \varphi_q) = 0$, also $\mathfrak{R}_n$ orthogonal zu $\mathfrak{R}_q$ ist. Umgekehrt folgt aus $\mathfrak{D}_S = \mathfrak{H}$, $| l_q | = 1$ und aus $(\varphi_n, \varphi_q) = 0$ für $n \neq q$, dass $S$ unitär ist: Für $f_1 \in \mathfrak{D}_S$, $f_2 \in \mathfrak{D}_S$ ist

$$f_1 = \varphi_{0,1} + \varphi_{1,1} + \cdots + \varphi_{k-1,1}, \qquad f_2 = \varphi_{0,2} + \varphi_{1,2} + \cdots + \varphi_{k-1,2},$$

$$\varphi_{q,1} \in \mathfrak{R}_q, \ \varphi_{q,2} \in \mathfrak{R}_q,$$

$$(Sf_1, Sf_2) = (l_0\varphi_{0,1} + l_1\varphi_{1,1} + \cdots, l_0\varphi_{0,2} + l_1\varphi_{1,2} + \cdots)$$

$$= \sum_{q=0}^{k-1} | l_q |^2 (\varphi_{q,1}, \varphi_{q,2}) = \sum_{q=0}^{k-1} (\varphi_{q,1}, \varphi_{q,2}) = (f_1, f_2).$$

Da nun $\mathfrak{D}_S = \mathfrak{H}$ ist, ist auch der Vorrat ("range") gleich $\mathfrak{H}$ (Satz IV), $S$ unitär.

Der Beweis von III ($\delta$) ergibt sich durch entsprechende Überlegungen.

## 4. Die Fragen der Umkehrbarkeit und des Spektrums beantwortet

Satz IV. *Sei $S$ von algebraischem Typ, $S_l = S - lI$. Wenn $l$ von allen Eigenwerten von $S$ verschieden ist, dann und nur dann ist $S_l$ umkehrbar, dann und nur dann der Vorrat ("range") von $S_l$ gleich dem Bereiche $\mathfrak{D}_S$ von $S$. Die Umkehrung $S_l^{-1}$ ist dann und nur dann beschränkt, wenn $S$ es ist.*

HILFSSATZ IVA. *Wenn in einer Transformation $S$ von algebraischem Typ kein Eigenwert Null ist, dann und nur dann ist $S$ umkehrbar, dann und nur dann der*

[4] C.f. M. H. Stone, Theorem 8.2.

*Vorrat gleich dem Bereiche* $\mathfrak{D}_S$. *Die Umkehrung* $S^{-1}$ *ist dann und nur dann stetig, wenn* $S$ *es ist.*

BEWEIS. Sei $k$ der Grad von $S$, sei kein Eigenwert Null,

$$P_k(Sf) = S^k f + a_{k-1}S^{k-1}f + \cdots + a_1 Sf + a_0 f = 0, \qquad f \in \mathfrak{D}_S, \tag{4.1}$$

dann ist $a_0 = (-1)^k l_0 l_1 \cdots l_{k-1} \neq 0$, für $g = Sf$ gehört $g$ auch zu $\mathfrak{D}_S$ (Def. B),

$$f = -a_0^{-1}(S^{k-1}g + a_{k-1}S^{k-2}g + \cdots + a_1 g), \tag{4.2}$$

also existiert $S^{-1}g = f$. Die rechte Seite hat aber für alle $g$ aus $\mathfrak{D}_S$ Sinn, für ein aus (4.2) bei beliebigem $g \in \mathfrak{D}_S$ bestimmtes $f$ folgt wegen $P_k(Sg) = 0$

$$Sf = -a_0^{-1}(S^k g + a_{k-1}S^{k-1}g + \cdots + a_1 Sg) = -a_0^{-1}(-a_0 g) = g. \tag{4.3}$$

Ist andrerseits $S$ umkehrbar, so gibt es keine von Null verschiedene Lösung $f$ von $Sf = 0$, also ist Null nicht Eigenwert.

Ist der Vorrat $\mathfrak{D}_S$, so muss z.B. auch eine Lösung $f$ von $Sf = \psi_q$ für irgendein von Null verschiedenes $\psi_q$ aus $\mathfrak{R}_q$ vorhanden sein. Aus $f = \varphi_0 + \varphi_1 + \cdots + \varphi_{k-1}$, $\varphi_q \in \mathfrak{R}_q$, folgt dann

$$\psi_q = Sf = l_0\varphi_0 + l_1\varphi_1 + \cdots + l_{k-1}\varphi_{k-1},$$

aus Hilfssatz Ia ($\gamma$) dann $\psi_q = l_q\varphi_q$; daher ist $l_q \neq 0$, kein Eigenwert Null.

Wenn $S$ stetig ist, $\| Sf \| \leqq B \| f \|$, und umkehrbar, folgt aus (4.2) sofort $\| S^{-1}g \| = \| f \| \leqq A \| g \|$; umgekehrt, wenn $\| S^{-1}g \| \leqq A \| g \|$ ist, folgt aus (4.1)

$$Sf + a_{k-1}f + a_{k-2}S^{-1}f + \cdots + a_0 S^{1-k}f = 0,$$

$$\| Sf \| = \| a_{k-1}f + a_{k-2}S^{-1}f + \cdots + a_0 S^{1-k}f \| \leqq B \| f \|.$$

Somit ist der Hilfssatz bewiesen. Sei nun $S_l = S - lI$, $l$ beliebig, dann haben $S$ und $S_l$ denselben Bereich, dieselben Eigenfunktionen, $S$ und $S_l$ sind beide stetig oder beide unstetig; seien $l_q'$ die Eigenwerte von $S_l$, so ist $l_q' = l_q - l$, $l_q = l_q' + l$, $S$ und $S_l$ haben daher (s. 4.4) denselben Grad, und die Eigenwerte von $S_l$ sind dann und nur dann sämtlich von Null verschieden, wenn $l$ von allen $l_q$ verschieden ist. Für alle $f$ aus $\mathfrak{D}_S$ ist:

$$P_k(Sf) = \left\{\prod_{q=0}^{k-1}(S - l_q I)\right\} f = \left\{\prod_{q=0}^{k-1}(S_l - (l_q - l)I)\right\} f = \bar{P}_k(S_l f) = 0. \tag{4.4}$$

So ergibt sich leicht der Beweis des allgemeinen Falles, des Satzes IV.

Mit Hilfe von Satz II folgt unschwer der

ZUSATZ IVA. *Ist* $S$ *vom allgebraischen Typ mit den Eigenwerten* $l_0, l_1, \cdots l_{k-1}$ *und* $S_{l_0} = S - l_0 I$, *so ist der Vorrat von* $S_{l_0}$ *die lineare Mannigfaltigkeit, welche durch die Vereinigungsmenge von* $\mathfrak{R}_1, \mathfrak{R}_2, \cdots \mathfrak{R}_{k-1}$ *bestimmt ist.*

**5. Satz V.** *Sei* $S$ *vom algebraischen Typ, Grad* $k$ *und beschränkt,* $\{\varphi_{q,n}\}$, $n = 0, 1, 2 \cdots$ *eine Funktionenfolge aus* $\mathfrak{R}_q$ ($q = 0, 1, \cdots, k-1$), *sei die Folge*

$\{\varphi_{p,n}\}(p = 0, 1, \cdots, k-1; n = 0, 1, 2, \cdots)$, *also* $\varphi_{0,0}, \varphi_{1,0}, \cdots, \varphi_{k-1,0}$; $\varphi_{0,1}, \varphi_{1,1}, \cdots, \varphi_{k-1,1}$; $\varphi_{0,2}, \varphi_{1,2}, \cdots, \varphi_{k-1,2}$; $\varphi_{0,3}, \cdots$ *ein in* $\mathfrak{D}_S$ *abgeschlossenes System. Dann ist die Folge* $\{\varphi_{q,n}\}$, $n = 0, 1, 2, \cdots$, *ein in* $\mathfrak{R}_q$ *abgeschlossenes System für jedes* $q$, $q = 0, 1, \cdots, k-1$.

HILFSSATZ VA. *Sei* $S$ *wie oben,* $\{\Phi_n\}$ *ein in* $\mathfrak{D}_S$ *abgeschlossenes System, d.h. wenn* $f$ *aus* $\mathfrak{D}_S$ *beliebig gegeben ist, sollen zu jedem* $\epsilon > 0$ *Zahlen* $a_0, a_1, \cdots, a_m$, $m \geqq 0$, *vorhanden sein der Art, dass* $\| f - a_0\Phi_0 - a_1\Phi_1 - \cdots - a_m\Phi_m \| \leqq \epsilon$ *ist. Dann ist die Folge* $\{X_n^{(q)}\} = \{Q_q(S\Phi_n)\}$ (s. 2.2), $n = 0, 1, \cdots$, *ein in* $\mathfrak{R}_q$ *abgeschlossenes System.*

Nach Hilfssatz Ia ($\alpha$) ist $X_n^{(q)}$ eine zu $l_q$ gehörige Eigenfunktion oder Null, die Transformation $Q_q(Sf)$ ist auch beschränkt, also $\| Q_q(Sf) \| \leqq A \| f \|$. Sei $\psi_q$ aus $\mathfrak{R}_q$ gewählt, $m, a_0, a_1, \cdots, a_m$ so bestimmt, dass $\psi_q - a_0\Phi_0 - a_1\Phi_1 - \cdots - a_m\Phi_m = \eta$, $\| \eta \| \leqq \epsilon/A$ ist. Hieraus folgt:

$$Q_q(S\psi_q) - a_0Q_q(S\Phi_0) - a_1Q_q(S\Phi_1) - \cdots - a_mQ_q(S\Phi_m) = Q_q(S\eta).$$

Aber $Q_q(S\psi_q)$ ist $\psi_q$ (s. 2.3), $Q_q(S\Phi_n)$ ist $X_n^{(q)}$, $\| Q_q(S\eta) \| \leqq A \| \eta \| \leqq \epsilon$, also

$$\| \psi_q - a_0X_0^{(q)} - a_1X_1^{(q)} - \cdots - a_mX_m^{(q)} \| \leqq \epsilon,$$

$\{X_n^{(q)}\}$ ist also ein in $\mathfrak{R}_q$ abgeschlossenes System.

Sei $\{\Phi_j\}$ nun die, nach Voraussetzung in $\mathfrak{D}_S$ abgeschlossene, Folge $\{\varphi_{p,n}\}$, $p = 0, 1, \cdots, k-1, n = 0, 1, 2, \cdots$, dann ist $Q_q(S\varphi_{p,n}) = 0$ oder $\varphi_{q,n}$ für $p \neq q$ bezw. $p = q$ (s. 2.3), also die Folge $\{\varphi_{q,n}\}$ ($q$ fest, $n = 0, 1, 2 \cdots$) identisch mit $\{X_j^{(q)}\}$ bis auf Nullelemente und daher ein in $\mathfrak{R}_q$ abgeschlossenes System.— Man beweist schliesslich unschwer:

ZUSATZ VB. *Wenn die Doppelfolge* $\{\varphi_{p,n}\}$ *des Satzes V ein vollständiges orthonormales System des als ein Hilbertscher Raum vorausgesetzten Bereiches* $\mathfrak{D}_S$ *ist, ist* $\{\varphi_{q,n}\}$, $q$ *fest, ein solches der abgeschlossenen linearen Mannigfaltigkeit* $\mathfrak{R}_q$.

6. SATZ VI. *Seien* $S$ *und* $T$ *Transformationen in* $\mathfrak{H}$ *von algebraischem Typ mit den gleichen Eigenwerten* $l_0, l_1, \cdots, l_{k-1}$, *seien* $\mathfrak{R}_q$ *bezw.* $\mathfrak{R}_q'$ ($q = 0, 1, \cdots, k-1$) *die entsprechenden Räume der Eigenfunktionen. Eine lineare Transformation* $W$ *in* $\mathfrak{H}$ *bildet dann und nur dann jedes* $\mathfrak{R}_q$ *auf* $\mathfrak{R}_q'$ *oder einen Teil von* $\mathfrak{R}_q'$ *ab, wenn ihr Bereich den von* $S$ *enthält und für alle* $f$ *aus* $\mathfrak{D}_S$ *ausserdem* $TWf$ *Sinn hat und* $WSf = TWf$ *ist.*

Dieser Satz liefert für involutorische Transformationen die sogenannten Beziehungen zwischen selbstreziproken Funktionen[5] und wird ganz entsprechend wie dort bewiesen (s. Verf. III).

---

[5] G. H. Hardy, and E. C. Titchmarsh, Proc. London Math. Soc. (2), 33 (1931), 225–32. E. C. Titchmarsh, *Introduction to the Theory of Fourier Integrals*, Oxford 1937; dort auch vollständige weitere Literaturangabe.

**7. Beispiele:** Mögen $H_n(x)$ bezw. $L_n^{(\alpha)}(x)$ die Hermiteschen bezw. Laguerreschen Polynome bedeuten, $\Phi_n$ bezw. $\Psi_n$ fortan stets folgende Funktionen:

$$(7.1)\qquad \Phi_n(x) = \frac{e^{-\frac{1}{2}x^2}H_n(x)}{(2^n n\cdot\sqrt{\pi})^{\frac{1}{2}}}; \qquad H_n(x) = (-1)^n e^{x^2}\frac{d^n e^{-x^2}}{dx^n},$$

$$(7.2)\qquad \Psi_n^{(\alpha)}(x) = \left(\frac{2n!e^{-x^2}}{\Gamma(n+\alpha+1)}\right)^{\frac{1}{2}} x^{\alpha+\frac{1}{2}}L_n^{(\alpha)}(x^2); \quad L_n^{(\alpha)}(x) = \sum_{r=0}^{n}\binom{n+\alpha}{n-r}\frac{(-x)^r}{r!},$$

$$n = 0, 1, 2, 3, \cdots; \text{ sei stets } \Re(\alpha) > -1.$$

A. Die Fourier-Transformation $g = S_{(h)}f$, $f(x_1, \cdots, x_h) \in \mathfrak{L}_2^{(h)}(-\infty, \infty)$, $h \geqq 1$,

$$g(x_1, x_2, \cdots, x_h)$$

$$= (2\pi)^{-\frac{1}{2}h} \operatorname*{l.i.m.}_{m_1, m_2, \cdots \to \infty} \int_{-m_1}^{m_1} \cdots \int_{-m_h}^{m_h} e^{i(t_1x_1+\cdots+t_hx_h)} f(t_1, \cdots, t_h)\, dt_1 \cdots dt_h.$$

Bekanntlich ist $S_{(h)}$ unitär, also auch stetig und abgeschlossen,

$$(7.3)\qquad S_{(1)}\Phi_n = (i)^n\Phi_n \qquad (h = 1),$$

$$(7.4)\qquad S_{(h)}^4 f = If = f.$$

Die Nullstellen des Polynoms $P_4(z) = z^4 - 1$ sind $l_q = (i)^q$, $q = 0, 1, 2, 3$, also treten höchstens die 4 Eigenwerte $i^q$ auf. Nun sind die Funktionen

$$\Phi(x_1, \cdots, x_h\,;\, n_1, \cdots, n_h) = \Phi_{n_1}(x_1)\Phi_{n_2}(x_2)\Phi_{n_3}(x_3)\cdots\Phi_{n_h}(x_h),$$

wenn $n_1, n_2, \cdots, n_h$ unabhängig alle ganzen nicht negativen Zahlen durchlaufen, ein vollständiges orthonormales System des Raumes $\mathfrak{L}_2^{(h)}$; wegen (7.3) ist

$$S_h\Phi(x_1, \cdots, x_h\,;\, n_1, \cdots, n_h) = i^{n_1+n_2+\cdots n_h}\Phi(x_1, \cdots, x_h\,;\, n_1, \cdots, n_h),$$

also treten alle 4 Eigenwerte auf, $S_{(h)}$ ist vom algebraischen Typ und Grad 4, $\Phi$ ist für $n_1 + n_2 + \cdots + n_h \equiv q \pmod 4$ eine zum Eigenwert $i^q$ gehörige Eigenfunktion. Jedes $\mathfrak{R}_q$ ist ein Hilbertscher Raum, da es nach III$\alpha$ eine abgeschlossene lineare Mannigfaltigkeit ist und es nicht bloss endlich viele linear unabhängige Elemente enthält. Es gelten alle oben bewiesenen Sätze, insbesondere ist die Folge

$$\{\Phi_{n_1}(x_1)\Phi_{n_2}(x_2)\cdots\Phi_{n_h}(x_h)\}, \qquad [n_1 + n_2 + \cdots + n_h \equiv q \pmod 4]$$

ein vollständiges orthonormales System des Hilbertschen Raumes $\mathfrak{R}_q$.[6]

Die Transformation $Q_q(Sf)$, welche $\mathfrak{L}_2^{(h)}$ auf $\mathfrak{R}_q$ projiziert, ist (s. 2.1)

$$Q_q(Sf) = \tfrac{1}{4}\{f + (-i)^q Sf + i^{2q}S^2f + (-i)^{3q}S^3f\}.$$

B. Die Hankelsche Transformation $g = Tf, f \in \mathfrak{L}_2(0, \infty)$ (s. 1).

---

[6] Der Fall $h = 1$, $q = 0$ ist für andere Räume bei E. Feldheim, Bull. Sci. Math. 2, 61 (1937), 10–18 behandelt. C.f. N. Wiener, *The Fourier integral* . . . (Cambridge 1933).

Da $T^2f - f = 0$ ist, ist hier $P_m(z) = z^2 - 1$, Nullstellen sind $l_0 = 1$, $l_1 = -1$. Beide Eigenwerte treten auf, $T$ ist also vom algebraischen Typ, Grad 2, denn

$$T\Psi_n^{(\alpha)} = (-1)^n \Psi_n^{(\alpha)}, \qquad n = 0, 1, 2, \cdots. \tag{7.5}$$

Durch $Q_q(Tf) = \frac{1}{2}\{f + (-1)^q Tf\}$ wird $\mathfrak{L}_2(0, \infty)$ auf $\mathfrak{R}_q$ projiziert. Bekanntlich ist die Folge $\Psi_n^{(\alpha)}$[7] ein in $\mathfrak{L}_2(0, \infty)$ abgeschlossenes System, daher sind $\{\Psi_{2n}^{(\alpha)}\}$ bezw. $\{\Psi_{2n+1}^{(\alpha)}\}$, $n = 0, 1, 2, \cdots$, nach Satz V abgeschlossene Systeme in den Hilbertschen Räumen $\mathfrak{R}_0$ bezw. $\mathfrak{R}_1$ der "selbst-" bezw. "schiefreziproken" Funktionen. Wenn $\alpha$ reell ist, dann und nur dann ist $T$ unitär, dann sind auch $\{\Psi_n^{(\alpha)}\}$ bezw. $\{\Psi_{2n}^{(\alpha)}\}$, $\{\Psi_{2n+1}^{(\alpha)}\}$ vollständige orthonormale Systeme von $\mathfrak{L}_2$ bezw. $\mathfrak{R}_0$, $\mathfrak{R}_1$.

C. Bedeute $((u))$ die Differenz zwischen $u$ und der nächsten ganzen Zahl, sei $r$ reell. Die Transformationen

$$g(x) = S_r f = C_r \operatorname*{l.i.m.}_{n\to\infty} \int_{-n}^{n} \exp\left[\frac{itx}{\sin 2\pi r} - \frac{i}{2}(x^2 + t^2)\cot 2\pi r\right] f(t)\, dt,$$

$$f(x) \in \mathfrak{L}_2(-\infty, \infty),\ 2r \text{ nicht ganz: } S_r f(x) = f(\pm x) \text{ für } r \equiv 0 \text{ bzw. } \tfrac{1}{2} \pmod 1. \tag{7.6}$$

$$C_r = (2\pi\,|\sin 2\pi r\,|)^{-1} \exp\left[\tfrac{1}{2} i\pi((\tfrac{1}{2} - 2r))\right].$$

$$g(x) = T_r f = c_r \operatorname*{l.i.m.}_{n\to\infty} \int_0^n J_\alpha\left(\frac{tx}{|\sin \pi r|}\right) \exp\left[-\frac{i}{2}(x^2 + t^2)\cot \pi r\right] (tx)^{\frac{1}{2}} f(t)\, dt,$$

$$f(x) \in \mathfrak{L}_2(0, \infty);\ r \text{ nicht ganz, } S_r = I \text{ für ganzes } r; \tag{7.7}$$

$$c_r = |\sin \pi r|^{-1} \exp\left[i\pi(1 + \alpha)((\tfrac{1}{2} - r))\right].$$

$$g(x) = U_r f = \frac{i}{2\pi}\frac{d}{dx}\int_0^1 \log\left|\frac{\cos \pi t - \cos \pi(x + 2r)}{\cos \pi t - \cos \pi(x - 2r)}\right| f(t)\, dt \tag{7.8}$$

$$+ \tfrac{1}{2} f(2r - x) + \tfrac{1}{2} f(2r + x),$$

$r$ reell; $f(x) \in \mathfrak{L}_2(0, 1)$, gerade und periodisch, Periode 2,

sollen die gemeinsame Bezeichnung $V_r$, die Folgen $\{\Phi_n\}$ bezw. $\{\Psi_n\}$ bezw. $\{1, \sqrt{2}\cos \pi x\ \sqrt{2}\cos 2\pi x, \cdots\}$ die Bezeichnung $\{F_n\}$ tragen. Für $r = 1/4$ ist $S_r$ die Fouriersche, für $r = 1/2$ ist $T_r$ die Hankelsche und $U_r$ die Transformation $g(x) = f(1 - x)$. In einer anderen Arbeit[8] werden nun folgende einfache Gesetze bewiesen: *Alle diese Transformationen existieren, sind, $T_r$ allerdings nur für reelles $\alpha$, unitär,*

$$V_0 = I, \qquad V_{r+1} = V_r;\ V_r V_s = V_{r+s};\ \text{also } V_r^{-1} = V_{-r};\ V_r^k = V_{kr}$$

---

[7] Das folgt, da $\Phi_n(\beta)$ $\{\Psi_n^{(\beta)}(x)\}$ für reelles $\beta$ ein vollständiges orthonormales System von $\mathfrak{L}_2(0, \infty)$ ist, für $\alpha = \beta + i\gamma$ leicht aus

$$L_n^{(\beta)}(x) = \sum_{s=0}^{n} \binom{n - i\gamma - 1 - s}{n - s} L_s^{(\alpha)}(x)$$

[8] Quart. J. of Math. (Oxford) 10 (1939), 45–59. Dort Beweis von (T.5).

*für beliebiges ganzes $k$*; seien $r = m/k$, $m$ und $k$ ganz, positiv und teilerfremd, so folgt

$$V_r^k = I \qquad \left(r = \frac{m}{k}\right).$$

Ferner ist $\exp(2i\pi rn)F_n = V_rF_n$. Daher ist $V_{m/k}$ vom algebraischen Typ, Grad $k$, die Eigenwerte sind $\exp(2i\pi qm/k)$, $q = 0, 1, \cdots, k-1$, nach Satz V ist die Folge $F_q, F_{q+k}, F_{q+2k}, \cdots$ ein im Hilbertschen Raume $\mathfrak{R}_q$ abgeschlossenes System, sogar für alle unitären $V$ ein vollständiges orthonormales System von $\mathfrak{R}_q$. Der Raum $\mathfrak{L}_2$ wird auf $\mathfrak{R}_q$ projiziert durch

$$Q_q(V_r f) = \frac{1}{k}\sum_{s=0}^{k-1}(e^{-2i\pi qr}V_r)^s f, \qquad \left(r = \frac{m}{k}\right).$$

Sei $k$ positiv und ganz, so ist $S_r$ für $r = (4k)^{-1}$ bezw. $T_r$ für $r = (2k)^{-1}$ eine $k$. Wurzel aus der Fourier- bezw. Hankel-Transformation, weil dann $S_r^k = S_{kr} = S_{1/4}$ bezw. $T_r^k = T_{kr} = T_{1/2}$ ist.

D. Satz VII. *Seien $\mathfrak{M}_0, \mathfrak{M}_1, \cdots, \mathfrak{M}_{k-1}$ beliebig gegebene lineare, linear unabhängige Mannigfaltigkeiten in $\mathfrak{H}$, $l_0, l_1, \cdots, l_{k-1}$ beliebige voneinander verschiedene endliche Zahlen. Dann gibt es stets genau eine Transformation von algebraischem Typ, welche genau die Eigenwerte $l_0, l_1, \cdots, l_{k-1}$ und als Räume der zugehörigen Eigenfunktionen $\mathfrak{M}_0, \mathfrak{M}_1, \cdots, \mathfrak{M}_{k-1}$ hat.*

Sei $\mathfrak{D}_s$ die durch Vereinigung aller Mengen $\mathfrak{M}_q$ bestimmte lineare Mannigfaltigkeit, dann ist sicher jedes $f \in \mathfrak{D}_s$ in der Form $f = f_0 + f_1 + \cdots + f_{k-1}$, $f_q \in \mathfrak{M}_q$, darstellbar, eindeutig wegen der linearen Unabhängigkeit der $\mathfrak{M}_q$. Man ordne nun $f$ folgende Funktion zu:

$$g = Tf = l_0f_0 + l_1f_1 + \cdots + l_{k-1}f_{k-1}. \tag{7.9}$$

Die so definierte Transformation $T$ ist sicher linear, es ist $Tf_q = l_qf_q$, die Schlussweise von (2.4) u.s.w. ergibt die Behauptung.

Sei z.B. $\mathfrak{H} = \mathfrak{L}_2(-\infty, \infty)$; $l_0, l_1, \cdots, l_{k-1}$ beliebig gegeben, $\mathfrak{M}_q$ sei der Hilbertsche Raum mit dem vollständigen orthonormalen System $\Phi_q, \Phi_{q+k}, \Phi_{q+2k}, \cdots$, dann ist die gewünschte Transformation, stetig nach Satz III,

$$g(x) = Tf = \sum_{q=0}^{k-1} l_q \sum_{n=0}^{\infty}(f, \Phi_{q+kn})\Phi_{q+kn}(x), \qquad f \in \mathfrak{H}, \tag{7.10}$$

welche sich durch folgenden Integraloperator darstellen lässt:

$$\begin{aligned} g(x) = {} & \frac{f(x)}{k}\sum_{s=0}^{k-1} l_s + \frac{f(-x)}{k}\sum_{s=0}^{k-1}(-1)^s l_s \\ & + \operatorname*{l.i.m.}_{n\to\infty}\int_{-n}^{n}\left[\sum_{s=0}^{k-1} l_s \sum_{r=1}^{k-1}{}' K_{r,s}(x,y)\right]f(y)\,dy, \end{aligned} \tag{7.11}$$

$$\begin{aligned} K_{r,s} = {} & \frac{1}{k}\left(2\pi\left|\sin\frac{2\pi r}{k}\right|\right)^{-1}\exp\left[i\pi\left\{\tfrac{1}{2}\left(\left(\frac{1}{2}-\frac{2r}{k}\right)\right) - \frac{2rs}{k}\right\}\right. \\ & \left. + i\left(\frac{xy}{\sin 2\pi r/k} - \frac{x^2+y^2}{2}\cot\frac{2\pi r}{k}\right)\right]. \end{aligned}$$

Für gerades $k$ ist hier in $\sum'$ das Glied mit $r = \frac{1}{2}k$, für ungerades $k$ ist das Glied $k^{-1}f(-x)\sum(-1)^r l_r$ fortzulassen. Man gewinnt (7.11) entsprechend wie (7.6), hier unter Benutzung einer leicht aus Mehlers Formel[9] für $|t| < 1$, ganzes positives $k$ und $\epsilon = \exp(2i\pi/k)$ beweisbaren Gleichung

$$\sum_{n \equiv a \pmod k}^{n \geqq 0} t^n \Phi_n(x)\Phi_n(y) = \frac{1}{k\sqrt{\pi}} \sum_{r=0}^{k-1} \frac{\epsilon^{-ra}}{(1 - t^2\epsilon^{2r})^{\frac{1}{2}}} \exp\left[\frac{4xyt\epsilon^r - (x^2 + y^2)(1 + t^2\epsilon^{2r})}{2(1 - t^2\epsilon^{2r})}\right].$$

THE UNIVERSITY EDGBASTON, BIRMINGHAM, ENGLAND.

---

[9] N. Wiener, l.c.; G. N. Watson, J. of London Math. Soc. 8 (1933), 194–9. Die Anregung zu dem letzten Beispiele verdanke ich Herrn H. Lewy, Berkeley.

*für beliebiges ganzes* $k$; seien $r = m/k$, $m$ und $k$ ganz, positiv und teilerfremd, so folgt

$$V_r^k = I \qquad \left(r = \frac{m}{k}\right).$$

Ferner ist $\exp(2i\pi rn)F_n = V_r F_n$. Daher ist $V_{m/k}$ vom algebraischen Typ, Grad $k$, die Eigenwerte sind $\exp(2i\pi qm/k)$, $q = 0, 1, \cdots, k-1$, nach Satz V ist die Folge $F_q, F_{q+k}, F_{q+2k}, \cdots$ ein im Hilbertschen Raume $\mathfrak{R}_q$ abgeschlossenes System, sogar für alle unitären $V$ ein vollständiges orthonormales System von $\mathfrak{R}_q$. Der Raum $\mathfrak{L}_2$ wird auf $\mathfrak{R}_q$ projiziert durch

$$Q_q(V_r f) = \frac{1}{k}\sum_{s=0}^{k-1}(e^{-2i\pi qr}V_r)^s f, \qquad \left(r = \frac{m}{k}\right).$$

Sei $k$ positiv und ganz, so ist $S_r$ für $r = (4k)^{-1}$ bezw. $T_r$ für $r = (2k)^{-1}$ eine $k$. Wurzel aus der Fourier- bezw. Hankel-Transformation, weil dann $S_r^k = S_{kr} = S_{1/4}$ bezw. $T_r^k = T_{kr} = T_{1/2}$ ist.

D. Satz VII. *Seien* $\mathfrak{M}_0, \mathfrak{M}_1, \cdots, \mathfrak{M}_{k-1}$ *beliebig gegebene lineare, linear unabhängige Mannigfaltigkeiten in* $\mathfrak{H}$, $l_0, l_1, \cdots, l_{k-1}$ *beliebige voneinander verschiedene endliche Zahlen. Dann gibt es stets genau eine Transformation von algebraischem Typ, welche genau die Eigenwerte* $l_0, l_1, \cdots, l_{k-1}$ *und als Räume der zugehörigen Eigenfunktionen* $\mathfrak{M}_0, \mathfrak{M}_1, \cdots, \mathfrak{M}_{k-1}$ *hat.*

Sei $\mathfrak{D}_s$ die durch Vereinigung aller Mengen $\mathfrak{M}_q$ bestimmte lineare Mannigfaltigkeit, dann ist sicher jedes $f \in \mathfrak{D}_s$ in der Form $f = f_0 + f_1 + \cdots + f_{k-1}$, $f_q \in \mathfrak{M}_q$, darstellbar, eindeutig wegen der linearen Unabhängigkeit der $\mathfrak{M}_q$. Man ordne nun $f$ folgende Funktion zu:

$$g = Tf = l_0 f_0 + l_1 f_1 + \cdots + l_{k-1} f_{k-1}. \tag{7.9}$$

Die so definierte Transformation $T$ ist sicher linear, es ist $Tf_q = l_q f_q$, die Schlussweise von (2.4) u.s.w. ergibt die Behauptung.

Sei z.B. $\mathfrak{H} = \mathfrak{L}_2(-\infty, \infty)$; $l_0, l_1, \cdots, l_{k-1}$ beliebig gegeben, $\mathfrak{M}_q$ sei der Hilbertsche Raum mit dem vollständigen orthonormalen System $\Phi_q, \Phi_{q+k}, \Phi_{q+2k}, \cdots$, dann ist die gewünschte Transformation, stetig nach Satz III,

$$g(x) = Tf = \sum_{q=0}^{k-1} l_q \sum_{n=0}^{\infty}(f, \Phi_{q+kn})\Phi_{q+kn}(x), \qquad f \in \mathfrak{H}, \tag{7.10}$$

welche sich durch folgenden Integraloperator darstellen lässt:

$$\begin{aligned} g(x) = {} & \frac{f(x)}{k}\sum_{s=0}^{k-1} l_s + \frac{f(-x)}{k}\sum_{s=0}^{k-1}(-1)^s l_s \\ & + \operatorname*{l.i.m.}_{n\to\infty}\int_{-n}^{n}\left[\sum_{s=0}^{k-1} l_s \sum_{r=1}^{k-1}{}' K_{r,s}(x,y)\right] f(y)\,dy, \end{aligned} \tag{7.11}$$

$$\begin{aligned} K_{r,s} = {} & \frac{1}{k}\left(2\pi\left|\sin\frac{2\pi r}{k}\right|\right)^{-1}\exp\left[i\pi\left\{\tfrac{1}{2}\left(\left(\frac{1}{2}-\frac{2r}{k}\right)\right) - \frac{2rs}{k}\right\}\right. \\ & \left. + i\left(\frac{xy}{\sin 2\pi r/k} - \frac{x^2+y^2}{2}\cot\frac{2\pi r}{k}\right)\right]. \end{aligned}$$

Für gerades $k$ ist hier in $\sum'$ das Glied mit $r = \frac{1}{2}k$, für ungerades $k$ ist das Glied $k^{-1}f(-x)\sum(-1)^r l_r$ fortzulassen. Man gewinnt (7.11) entsprechend wie (7.6), hier unter Benutzung einer leicht aus Mehlers Formel[9] für $|t| < 1$, ganzes positives $k$ und $\epsilon = \exp(2i\pi/k)$ beweisbaren Gleichung

$$\sum_{n\equiv a\,(\mathrm{mod}\,k)}^{n\geqq 0} t^n \Phi_n(x)\Phi_n(y) = \frac{1}{k\sqrt{\pi}} \sum_{r=0}^{k-1} \frac{\epsilon^{-ra}}{(1-t^2\epsilon^{2r})^{\frac{1}{2}}} \exp\left[\frac{4xyt\epsilon^r - (x^2+y^2)(1+t^2\epsilon^{2r})}{2(1-t^2\epsilon^{2r})}\right].$$

THE UNIVERSITY EDGBASTON, BIRMINGHAM, ENGLAND.

---

[9] N. Wiener, l.c.; G. N. Watson, J. of London Math. Soc. 8 (1933), 194–9.
Die Anregung zu dem letzten Beispiele verdanke ich Herrn H. Lewy, Berkeley.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ON THE EXISTENCE OF A MEASURE INVARIANT UNDER A TRANSFORMATION

BY J. C. OXTOBY AND S. M. ULAM

(Received April 12, 1939)

## 1. Introduction

Transformations which leave a measure function invariant are of importance in many branches of mathematics, notably in dynamics and in the theory of probability. It is therefore of some interest to investigate under what circumstances an invariant measure is possible. This may be considered part of the general problem of determining conditions under which there exists in a space a measure which is invariant under a group of transformations acting on the space. This problem has been solved only in special cases. Thus in case the space is a locally compact separable topological group, considered as acted upon by the group of right (or left) translations by its own elements, Haar's theorem[1] asserts the existence of an invariant measure. We consider the case of a general complete separable metric space acted on either by a group consisting of an automorphism and its powers, or by a one-parameter group of automorphisms. We shall set up a method which yields a finite invariant measure whenever such a measure is possible.

One must, of course, specify what measure functions are to be admitted. In all cases they will be required to be completely additive, defined at least for all Borel sets, with real values $\geqq 0$, and not identically zero. For the most part, we shall be concerned with finite measures, that is, measure functions in which the whole space has finite measure. Only in §4 shall we consider infinite measures. A measure is said to be invariant under a transformation $T$ if $m(TA)$ is defined and equal to $m(A)$ whenever $m(A)$ is defined. A measure is said to be invariant under a group of transformations if it is invariant under every transformation of the group.

In the case of a compact metric space, Kryloff and Bogoliouboff[2] have shown that every automorphism (that is, one-to-one bicontinuous transformation), and every one-parameter continuous group of automorphisms, possesses a finite

[1] A. Haar, *Der Massbegriff in der Theorie der kontinuerlichen Gruppen*, Annals of Math. (2), *34* (1933) pp. 147–169. See also the note by S. Banach in Saks, *Theory of the Integral*, Warsaw-Lwów 1937, pp. 314–319. Also J. von Neumann, *The uniqueness of Haar measure*, Recueil mathématique Moscou, (1), vol. 43 (1936).

[2] N. Kryloff and N. Bogoliouboff, *La théorie générale de la mesure dans son application à l'étude des systèmes dynamiques de la mécanique non linéaire*, Annals of Math. (2), *38* (1937) pp. 65–113. Theorem 1, p. 92, states the result for a continuous group, and the same considerations apply to a single automorphism.

invariant measure. But in general, the existence of such a measure imposes a restriction on the transformation, and even in the compact case the only invariant measures may be quite trivial ones, confined to a finite set of points. By using a somewhat more general method than that of Kryloff and Bogolioubboff, we shall obtain a theorem which contains their result as a corollary, and shall also find necessary and sufficient conditions for the existence of non-trivial invariant measures.

## 2. Finite measures invariant under a transformation

THEOREM 1: *Let $T$ be an automorphism of a complete separable metric space $E$. In order that there exist a finite invariant measure in $E$ it is necessary and sufficient that for some point $p$ and compact set $C \subset E$, we have*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f_C(T^k p) > 0,$$

*where $f_C$ is the characteristic function of $C$. It is sufficient that the limit superior be positive.*

In words, the condition means that there exists a compact set some point of which returns with positive frequency (or superior frequency) under iteration of $T$.

Suppose such a measure exists. If $m(A)$ is any finite measure in a complete separable space, defined at least for Borel sets, there exists a compact set $C$ with positive measure.[3] Since the measure is assumed invariant under $T$, it follows from the ergodic theorem of Birkhoff[4] that the limit

$$f^*(p) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f_C(T^k p)$$

exists for almost all $p$, is measurable $(m)$, and that

$$\int_E f^*(p)\, dm(p) = m(C).$$

Hence the integrand must be defined and positive for at least one point $p$.

To prove sufficiency, it is convenient to make use of a notion of generalized limit due to Mazur and Banach. Namely, there exists a real-valued functional Lim $\xi_n$, defined for all bounded sequences $\{\xi_n\}$ of real numbers, such that

1) Lim $(a\xi_n + b\eta_n) = a$ Lim $\xi_n + b$ Lim $\eta_n$ $\quad a, b$ real

2) Lim $\xi_n \geqq 0$ if $\xi_n \geqq 0$ for $n = 1, 2, \cdots$

[3] S. Ulam, *Sur la mesure dans un espace sèparable et complet*, to appear in Comptes Rendus (Paris). The proof runs briefly as follows. Let $x_1, x_2, \cdots$ be a sequence of points dense in $E$. Let $S_n^k$ denote the closed sphere with center $x_n$ and radius $1/k$, and let $F_N^k = \sum_{n=1}^{n=N} S_n^k$. Suppose $0 < \epsilon < m(E)$ given. Define successively $N_1, N_2, \cdots$ where $N_k$ is the least positive integer such that $m(\prod_1^k F_{N_i}^i) > m(E) - \epsilon$. The closed set $C = \prod_1^\infty F_{N_i}^i$ is totally bounded, therefore compact, and $m(C) \geqq m(E) - \epsilon$.

[4] See e. g. E. Hopf, *Ergodentheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Berlin 1937, §14.

3) $\operatorname{Lim} \xi_{n+1} = \operatorname{Lim} \xi_n$

4) $\liminf_{n\to\infty} \frac{1}{n}(\xi_1 + \cdots + \xi_n) \leqq \operatorname{Lim} \xi_n \leqq \limsup_{n\to\infty} \frac{1}{n}(\xi_1 + \cdots + \xi_n)$.

The generalized limit is thus an extension of the limit by first means. In addition, it can be so defined that for any prescribed bounded sequence $\{\xi_n^0\}$ we have

5) $\operatorname{Lim} \xi_n^0 = \limsup_{n\to\infty} \frac{1}{n}(\xi_1^0 + \cdots + \xi_n^0)$.

The existence of a generalized limit with these properties is an immediate consequence of a theorem of Banach on extension of linear functionals.[5] We shall take $\xi_n^0 = f_C(T^n p)$, so that under our hypotheses $\operatorname{Lim} f_C(T^n p) > 0$. For every open set $G \subset E$ define $F(G) = \operatorname{Lim} f_G(T^n p)$. Following the procedure of Carathéodory, for every set $A \subset E$ define $m^*(A) = \inf \sum_1^\infty F(G_n)$, taking all sequences of open sets $G_n$ such that $A \subset \sum_1^\infty G_n$. The resulting set function is then an outer measure in the sense of Carathéodory, and hence defines a completely additive measure whose domain of definition includes all Borel sets. The measure is invariant under $T$ in virtue of condition 3), it is always $\leqq 1$ since $F(E) = 1$. Furthermore $m(C) > 0$, because any covering of the compact set $C$ contains a finite subfamily which covers $C$, and from the linearity of the functional Lim $\xi_n$ it follows that $m^*(C) \geqq \operatorname{Lim} f_C(T^n p) > 0$. Hence $m(E) > 0$, and the measure can be normalized so that $m(E) = 1$. It may be remarked that the set function $m^*(A)$ could be defined starting with an arbitrary point $p$. The sufficient condition stated in the theorem merely plays the rôle of insuring that the resulting measure be not identically zero.

If the space is compact, the condition is trivially satisfied by taking $C = E$ and an arbitrary point $p$, so that in this case an invariant measure always exists, as was shown by Kryloff and Bogoliouboff. The condition is also satisfied if $p$ is taken to be a periodic point and $C$ the set of its images. But in this case the measure obtained is quite trivial, being confined to $p$ and its images. Even in the compact case, however, the only finite invariant measures may be confined to a finite set of points, as is seen by considering the automorphism $Tx = x^2$ of the interval $0 \leqq x \leqq 1$. To obtain a condition for the existence of a non-trivial invariant measure, we distinguish two cases according as there are countably or uncountably many periodic points. We shall see that in the latter case a non-trivial invariant measure always exists, and in the former case a condition similar to that given in Theorem 1 is necessary and sufficient.

Suppose first that there are non-denumerably many periodic points. Let $E_n$, $n = 1, 2, \cdots$, be the set of points $p$ such that $T^n p = p$. At least one of the sets $E_n$ must be non-denumerable, since their union is. Let $E_N$ be the first such set. Then the set $E_N - \sum_1^{N-1} E_n$ is a closed, non-denumerable subset of a complete separable space, and hence, by the theorem of Cantor-Bendixson,

[5] Banach, *Théorie des opérations linéaires*, Warsaw 1932, p. 27 Theorem 1. In the terminology there used one need merely take $p(\{\xi_n\}) = \limsup_{n\to\infty} \frac{1}{n}(\xi_1 + \cdots + \xi_n)$, and $f(\{t\xi_n^0\}) = t\,p(\{\xi_n^0\})$ in the linear manifold determined by the element $\{\xi_n^0\}$.

contains a non-void perfect subset. This, in turn, contains a subset $C$ homeomorphic to the Cantor set.[6] Let $m_1(A)$ be a finite measure in $C$ which is zero for points.[7] The measure $m(A) = \sum_1^N m_1(C \cdot T^k A)$, defined for all Borel sets, is a finite measure, zero for points, and invariant under $T$. The measure is, in fact, confined to $C$ and its $N - 1$ disjoint images.

Suppose now that there are only countably many periodic points. The complementary invariant set $E_1$ of non-periodic points is $G_\delta$, and therefore homeomorphic to a complete space $E_1^*$.[8] Let $T_1$ denote the transformation $T$ considered as operating only within $E_1$, and let $T_1^*$ be the corresponding automorphism of $E_1^*$. A non-trivial measure in $E$ must be confined to $E_1$, since the rest of the space is countable. Thus $T$ will admit a non-trivial invariant measure if and only if $T_1^*$ does. But a measure invariant under $T_1^*$ is necessarily zero for points, since a non-periodic point cannot have positive measure if the measure of the whole space is to be finite. Thus Theorem 1 applies to $T_1^*$, and since the condition stated there holds in $E_1^*$ if and only if it holds in $E_1$, our conclusion can be stated thus,

THEOREM 2: *In order that an automorphism $T$ of a complete separable metric space $E$ admit a finite invariant measure which is zero for points, it is necessary and sufficient that one of the following conditions hold,*

1. *$T$ has non-denumerably many periodic points.*

2. *There is a compact set $C$ consisting of non-periodic points some one of which returns to $C$ with positive frequency (or superior frequency) under iteration of $T$.*

### 3. Finite measures invariant under a one-parameter group of transformations

The above methods can be adapted to the treatment of steady flows as well as transformations. By a steady flow we shall mean a one-parameter group of automorphisms $T_\lambda x$, $-\infty < \lambda < +\infty$, of $E$ such that $T_\lambda T_\mu x \equiv T_{\lambda+\mu} x$, $T_0 X \equiv x$. We shall assume further that the dependence of $T_\lambda x$ upon $\lambda$ is Borel measurable for each fixed $x$. In other words, for each $x$ and each closed set $F \subset E$ the set of numbers $\lambda$ such that $T_\lambda x \in F$ is a Borel subset of the real number system. From these assumptions it follows that $T_\lambda x$ is a Borel measurable function of $\lambda$ and $x$ simultaneously.[9] It is therefore measurable in the sense of Hopf[10] with respect to any Borel measure, and the ergodic theorem can be applied in any such invariant measure.

THEOREM 3: *Let $T_\lambda x$ be a steady flow (in the sense just defined) of a complete separable metric space $E$ into itself. There exists a finite invariant measure in $E$*

---

[6] See e.g. Kuratowski, *Topologie* I, Warsaw-Lwów 1933, p. 228.

[7] Such a measure may conveniently be defined by mapping $C$ homeomorphically onto a Cantor set of Lebesgue measure one on the interval $0 \leqq x \leqq 2$ and taking the relative Lebesgue measure. It may be assumed further that the measure is positive for non-void relatively open subsets, a remark we shall use later.

[8] See e.g. Kuratowski, op. cit., p. 200.

[9] See e.g. Kuratowski, op. cit., p. 180.

[10] E. Hopf, op. cit., p. 9, Definition 3.4.

*if and only if for some point $p$ and compact set $C \subset E$ the limit (or limit superior) as $t \to \infty$ of the expression $\frac{1}{t}\int_0^t f_C(T_\lambda p)\, d\lambda$ is positive.*

The necessity of the condition follows immediately from the ergodic theorem and the existence of a compact set of positive measure, just as in the proof of Theorem 1. To prove sufficiency, we define a generalized limit Lim $f(\lambda)$ for all bounded Lebesgue measurable functions $f(\lambda)$, $-\infty < \lambda < +\infty$, fulfilling the conditions,[11]

1) Lim $[af(\lambda) + bg(\lambda)] = a$ Lim $f(\lambda) + b$ Lim $g(\lambda)$ $\quad a, b$ real
2) Lim $f(\lambda) \geqq 0$ if $f(\lambda) \geqq 0$
3) Lim $f(\lambda + \lambda_0) =$ Lim $f(\lambda)$ $\quad \lambda_0$ real
4) $\liminf_{t\to\infty} \frac{1}{t}\int_0^t f(\lambda)\, d\lambda \leqq$ Lim $f(\lambda) \leqq \limsup_{t\to\infty} \frac{1}{t}\int_0^t f(\lambda)\, d\lambda$
5) Lim $f_0(\lambda) = \limsup_{t\to\infty} \frac{1}{t}\int_0^t f_0(\lambda)\, d\lambda$ where $f_0(\lambda) = f_C(T_\lambda p)$.

We define $F(G) =$ Lim $f_G(T_\lambda p)$ for every open set $G \subset E$, and $m^*(A) = \inf \sum_1^\infty F(G_n)$ for all sequences of open sets $G_n$ whose union contains $A$. By an argument exactly similar to that in the proof of Theorem 1, we conclude that $m^*(A)$ is a Carathéodory outer measure which defines a finite measure invariant under the group $T_\lambda$.

## 4. Infinite invariant measures

A simple example of a transformation which admits no finite invariant measure is the automorphism $Tx = x + 1$ of the real number system. A more interesting example is the following. Let $T$ be a rotation of the circumference of the unit circle through an irrational angle. Let $C$ be a nowhere dense perfect set on $E$ with positive linear measure. The set $E_1 = E - \sum_{-\infty}^{+\infty} T^k C$ is then an invariant set of measure zero. Since it is $G_\delta$, it may be supposed re-metrized so as to be complete. Let $T_1$ be the transformation $T$ considered as an automorphism of $E_1$. $T_1$ admits no finite invariant measure, for such a measure would yield at once a measure in $E$ invariant under $T$ and positive for the set $E_1$. But the ordinary linear measure in $E$ is the *only* finite measure invariant under $T$, and in this measure $E_1$ has measure zero.

The first of these examples, of course, admits an infinite invariant measure, and one may ask whether such a measure always exists. We proceed to show that this is the case, and indeed that the measure may be made to satisfy certain additional requirements,

THEOREM 4: *Let $T$ be an automorphism of a metric space $E$, complete, separable, and dense in itself. There exists in $E$ a finite or infinite measure $m(A)$, which is invariant under $T$, defined for Borel sets, zero for points, positive (possibly infinite) for non-void open sets, and such that there is a set $A_0$ of finite measure*

[11] See footnote 5. Here we take $p[x(\lambda)] = \limsup_{t\to\infty} \frac{1}{t}\int_0^t x(\lambda)\, d\lambda$ and $f[tx_0(\lambda)] = t\, p[x_0(\lambda)]$ in the linear manifold determined by $x_0(\lambda)$.

*whose images* $T^k A_0$, $k = -\infty, \cdots, +\infty$, *are all disjoint and together exhaust all but a finite amount of the measure in* $E$.[12]

Let us prove first of all that if $S$ is any open sphere in which non-periodic points are dense, we can find a set $C \subset S$ which is homeomorphic to the Cantor set and whose images under powers of $T$ and $T^{-1}$ are all disjoint. Let us consider the open set $E_1 = \sum_{-\infty}^{+\infty} T^k S$ as our space. This will likewise be separable, dense in itself, and can be re-metrized so as to be complete. In it, non-periodic points form a dense $G_\delta$ set, therefore residual, and therefore non-denumerable in every neighborhood. We wish to define closed spheres $S_{i_1 \cdots i_n}$; $i_1, \cdots, i_n = 1, 2$; $n = 1, 2, \cdots$, such that 1) the sets $T^k S_{i_1 \cdots i_n}$, $k = 0, \pm 1, \cdots, \pm(n-1)$; $i_1, \cdots, i_n = 1, 2$ are disjoint, 2) $S_{i_1 \cdots i_n} \subset S_{i_1 \cdots i_{n-1}}$, and 3) $S_{i_1 \cdots i_n}$ has radius less than $1/n$. This is easily done step by step. $S_1$ and $S_2$ may be taken to be any two disjoint closed spheres of radius less than one. Suppose $S_{i_1 \cdots i_{n-1}}$, $i_1, \cdots, i_{n-1} = 1, 2$, already defined. In the interior of each of these spheres choose two points $x_{i_1 \cdots i_n}$, $i_n = 1, 2$, such that the $2^n$ points $x_{i_1 \cdots i_n}$ are distinct together with all of their images. This can be done, since, as we have seen, non-periodic points are non-denumerable in every sphere. Any sufficiently small spheres about the points $x_{i_1 \cdots i_n}$ will serve to define the spheres $S_{i_1 \cdots i_n}$. From the conditions 1), 2), and 3) it follows that the set

$$C = \prod_{n=1}^{\infty} \sum_{i_1, \cdots, i_n = 1,2} S_{i_1 \cdots i_n}$$

is homeomorphic to the Cantor set and that all its images are disjoint.[13]

We are now ready to prove the theorem. Let $S_1, S_2, \cdots$ be a sequence of open spheres which constitute a base for open sets in $E$. Let $S_{k_1}, S_{k_2}, \cdots$ be the subsequence of all spheres $S_n$ in which non-periodic points are dense, and let $S_{l_1}, S_{l_2}, \cdots$ be the subsequence of spheres $S_n$ which consist of periodic points only. These two subsequences, of which one or the other may be void, together constitute a base for open sets in $E$. For consider any sphere $S_n$. If the periodic points in it form a set of first category in $E$, it belongs to the subsequence $S_{k_i}$, and otherwise it contains one of the spheres $S_{l_i}$. For the present let us assume that neither subsequence is void. Let $C_1$ be a Cantor set contained in $S_{k_1}$ whose images are all disjoint. Supposing $C_1, C_2, \cdots, C_{n-1}$ defined, let $C_n$ be a Cantor set with disjoint images and contained in the first

[12] The condition that the space be dense in itself is clearly necessary, since an isolated point is itself an open set. This assumption can be dropped if it is required that the measure be positive only for non-denumerable open sets, but then it must be explicitly assumed that the space is not countable. It may be remarked that non-void open sets may necessarily have infinite measure. In the case of the automorphism $T_1$ of the space $E_1$ just considered, every non-void open set has a finite number of images which cover the space, and therefore must have infinite measure. In this space no open set is compact, but one cannot strengthen the theorem even to require that compact open sets have finite measure, as is seen again by the example $Tx = x^2$ on the interval $0 \leqq x \leqq 1$.

[13] From what has just been proved it follows that there exists a Cantor set on the circumference of the circle whose images under a given irrational rotation are all disjoint.

sphere $S_{k_i}$ which overlaps no image of $C_1, \cdots, C_{n-1}$. We thus arrive at a finite or infinite sequence of sets $C_i$ which are disjoint together with all their images. Let $m_i(A)$ be any normalized measure in $C_i$ which is zero for points and positive for non-void relatively open subsets. The measure

$$m_0(A) = \sum_{k=-\infty}^{+\infty} \sum_i \frac{1}{2^i} m(T^k A \cdot C_i)$$

will be an infinite invariant measure, defined for Borel sets in $E$, zero for points and positive for all $S_{k_i}$. Now let $G_i = \sum_{-\infty}^{+\infty} T^k S_{l_i}$. This open invariant set may be considered a complete space, and since periodic points are non-denumerable in it, we can apply Theorem 2 and get a normalized invariant measure $\mu_i(A)$ which is zero for points. The measure $\mu(A) = \sum_1^\infty 2^{-i} \mu_i(A \cdot G_i)$, defined for Borel sets, will be finite, zero for points, positive for all $S_{l_i}$, and invariant under $T$. Finally, the measure $m(A) = m_0(A) + \mu(A)$ will satisfy all requirements of the theorem, with $A_0 = \sum C_i$. If the sequence $S_{l_i}$ is void, the measure $m_0(A)$ alone suffices. If the sequence $S_{k_i}$ is void, the measure $\mu(A)$ suffices, with $A_0$ taken to be the void set.

SOCIETY OF FELLOWS, HARVARD UNIVERSITY.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ON AN INEQUALITY OF MARCEL RIESZ[0]

BY L. C. YOUNG

(Received February 13, 1939)

## 1. Introduction

The object of this note is to give a new proof of the inequality of Marcel Riesz.[1] In its original statement, this inequality, which has important applications in the theory of Fourier series and in the general theory of linear operations, concerns a bilinear form. We prefer the equivalent statement[2] as a theorem concerning the maximum

$$M_{\alpha\beta} = \operatorname*{Max}_{x} \frac{F_\beta^*(x)}{F_\alpha(x)} \tag{1.1}$$

of the ratio of two expressions, $F_\beta^*(x)$ and $F_\alpha(x)$ defined when $0 \leqq \alpha \leqq 1$ and $0 \leqq \beta \leqq 1$, each of which may be regarded as a kind of generalized "magnitude" of the $n$-dimensional vector $x$.

In the form in which we shall prove it, the theorem is made up of two parts:

(i) *a general* inequality involving several kinds of perfectly general "magnitudes" of the vector $x$ (the inequality (3.4) below).

(ii) *a special* property of the particular expressions $F_\alpha(x)$ and $F_\beta^*(x)$ with which Marcel Riesz's theorem is concerned (the property stated in (5.2) and (5.5) below). These particular expressions, which we shall speak of as "*Hölder functions*," are defined by the relations

$$F_\alpha(x) = \begin{cases} [S_{1/\alpha}(x)]^\alpha & \text{when } 0 < \alpha \leqq 1, \\ \lim\limits_{\alpha=0} [S_{1/\alpha}(x)]^\alpha & \text{when } \alpha = 0.[3] \end{cases} \tag{1.2}$$

$$F_\beta^*(x) = F_\beta(x \cdot A) \qquad (0 \leqq \beta \leqq 1) \tag{1.3}$$

---

[0] Since this paper was written, the author's attention has been drawn to an extremely important extension of M. Riesz's original theorem in a different direction from that of the consideration of the present paper. Cf. G. O. Thorin, "*An extension of a convexity theorem due to* M. Riesz", Kungl. Fysiografiska Sällskapets. I, Lund Förhandlinger, Bd. 8, No. 14 (9 Mar. 1938).

[1] Cf. M. Riesz, *Acta Mathematica* 49 (1927), pp. 465–497; Hardy, Littlewood, and Polya, *Inequalities*, pp. 214–221; and Zygmund, *Trigonometrical series*, pp. 192–200.

[2] Actually this is a little more general. The original form of the theorem would correspond to the case in which the matrix $A$ [in (1.3) below] fulfils additional conditions which render it equivalent to a complex $N$-dimensional matrix, where $N = \frac{1}{2}n$.

[3] For the existence of this limit, cf. Hardy, Littlewood and Polya, loc. cit.

where $A$ is a square $n$-dimensional matrix and where

$$S_r(x) = \sum_{h=1}^{2N} |x_{2h-1} + ix_{2h}|^r \quad \text{when} \quad r > 0, \tag{1.4}$$

the dimension $n$ of the vector $x$ being now restricted to be *even* and equal to $2N$. [Actually, slightly different ways of choosing $S_r(x)$ are possible[4] and these give rise to minor variants of the theorem.]

With these definitions, Marcel Riesz's theorem asserts that

(1.5) *The expression*

$$\log M_{\alpha\beta}$$

*is a convex function of* $\alpha$, $\beta$ *in the triangle* $0 \leqq \beta \leqq \alpha \leqq 1$.

By combining (i) and (ii) we obtain this theorem apart from the usual minor simplifications which are permissible by continuity.[5] More precisely we obtain the following assertion in the case in which $M_{\alpha\beta}$ is defined by (1.1)–(1.4) where we now suppose that $A$ is a matrix *with non-vanishing determinant*:[6]

(1.6) *Given any two points* $(\alpha_1, \beta_1)$ *and* $(\alpha_2, \beta_2)$ *of the triangle*

(1.7) $$0 < \beta < \alpha < 1,$$

*there exists on the open segment*

(1.8) $$\alpha = t\alpha_1 + (1-t)\alpha_2, \qquad \beta = t\beta_1 + (1-t)\beta_2, \quad (0 < t < 1),$$

*which joins* $(\alpha_1, \beta_1)$ *and* $(\alpha_2, \beta_2)$, *at least one point* $(\alpha, \beta)$ *such that*

(1.9) $$M_{\alpha\beta} \leqq (M_{\alpha_1\beta_1})^t (M_{\alpha_2\beta_2})^{1-t}.$$

## 2. Notions connected with magnitude of a vector

In the sequel we employ the usual vector notation: $x$ and $y$ denote the vectors $(x_1, \cdots, x_n)$ and $(y_1, \cdots, y_n)$, $x + y$ denotes their *sum* $(x_1 + y_1, \cdots, x_n + y_n)$, $x \cdot y$ their *scalar* product, the number $x_1y_1 + \cdots + x_ny_n$; while for *real* $t$, $tx$ denotes the vector $(tx_1, \cdots, tx_n)$. We write, further, 0 for $(0, \cdots, 0)$, $x^2$ for $x \cdot x$.

The "*magnitude*" of a vector $x$, just like the "distance" of two points $x$ and $y$, is to some extent an arbitrary notion which we need not link in any way with the theorem of Pythagoras. Following Minkowski, any function $F(x)$ may be interpreted as the magnitude of the vector $x$, if

$$\text{(2.1)} \quad \begin{cases} \text{(i)} \ F(x) > 0 & \text{when} \quad x \neq 0, \\ \text{(ii)} \ F(tx) = tF(x) & \text{when} \quad t \geqq 0, \\ \text{(iii)} \ F(x) + F(y) \geqq F(x + y). \end{cases}$$

[4] We require only (4.1) and (4.2) below, and homogeneity of degree $r$, together with the condition that (1.2) defines a function subject to (2.1) for $0 \leqq \alpha \leqq 1$.

[5] Hardy, Littlewood and Polya, loc. cit.

[6] In the rest of this note this hypothesis about the matrix $A$ will be made wherever $A$ occurs.

Any such a function is termed[7] also *function of distance* of a convex body $K$ containing the origin, and $K$ is the set of vectors $x$ such that $F(x) \leqq 1$.

The validity of (2.1) when $F(x)$ is the Hölder function (1.2) is little more than a restatement of "Minkowski's inequality."[8] Similarly (2.1) holds when $F(x)$ is the Hölder function (1.3), provided that[9] the matrix $A$ has a non-vanishing determinant.

With the function $F(x)$ there is associated a second function $G(y)$, called its *polar function*, defined by the relation

$$G(y) = \operatorname*{Max}_{x} \frac{x \cdot y}{F(x)}. \tag{2.2}$$

In the theory of convex bodies,[10] the function $G(y)$ is known as the "*Stützfunktion*" of the convex body $K$. It may be defined geometrically by means of the transformation of *reciprocal polars* with respect to the unit sphere $x^2 = 1$.

The notion of polar function is due to Minkowski who showed[11] that $G(y)$ *fulfils the same relations* (2.1) *as the function* $F(x)$, and that the relationship of the functions $F(x)$, $G(y)$ is a *symmetrical*[12] one, a fact which is almost evident from the connection with reciprocal polars. It follows that

$$F(x) = \operatorname*{Max}_{y} \frac{x \cdot y}{G(y)}. \tag{2.3}$$

Finally, we observe that either of the relations (2.2), (2.3) implies

$$x \cdot y \leqq F(x)G(y). \tag{2.4}$$

The inequality, together with its converses (2.2) and (2.3), is implicitly contained in the work of Minkowski. Its first explicit use, as an inequality, in this general form, is due to Mahler,[13] who makes important applications to the theory of numbers. We shall call it the *Minkowski-Mahler inequality*.

It follows at once that $M_{\alpha\beta}$, defined by (1.1), is also given by

$$M_{\alpha\beta} = \operatorname*{Max}_{y} \frac{G_\alpha(y)}{G^*_\beta(y)}, \tag{2.5}$$

---

[7] Cf. Bonnesen and Fenchel, *Theorie der konvexen Körper*, pp. 21–23.

[8] Cf. Hardy, Littlewood and Polya, pp. 30, 31.

[9] This restriction is needed for the validity of (2.1) (i).

[10] Cf. Bonnesen and Fenchel, loc. cit., pp. 23–28 and Mahler.[13]

It is easy to see that, by homogeneity of $F(x)$ [i.e. by the relation (2.1) (ii)], the definition (2.2) of $G(y)$ given in the text is equivalent to what Bonnesen and Fenchel call the "maximum property" of the Stützfunktion [cf., loc. cit., p. 24, lines 3–5].

[11] Cf. Bonnesen and Fenchel, loc. cit., p. 24.

[12] Ibidem, p. 28.

[13] Mahler, *Über polare convexe Körper*, Časopis, Praha, (not yet appeared).

Dr. Mahler very kindly communicated his results to the writer while they were still unpublished and made a number of important suggestions regarding the present note.

where $G_\alpha(y)$ and $G^*_\beta(y)$ are the polar functions of $F_\alpha(x)$ and $F^*_\beta(x)$ respectively. In fact, by (2.2) and (2.3),

$$\operatorname*{Max}_x \frac{F^*_\beta(x)}{F_\alpha(x)} = \operatorname*{Max}_x \operatorname*{Max}_y \frac{x \cdot y}{F_\alpha(x) G^*_\beta(y)} = \operatorname*{Max}_y \frac{G_\alpha(y)}{G^*_\beta(y)}.$$

If we restrict $F_\alpha(x)$ and $F^*_\beta(x)$ to be[14] the Hölder functions (1.2) and (1.3),

$$G_\alpha(y) = F_{1-\alpha}(y), \qquad G^*_\beta(y) = G_\beta(A_y^{-1}) \tag{2.6}$$

where $A^{-1}$ is the inverse matrix to $A$. The second of these formulae is an immediate consequence of the definition (2.2) when we make the substitution

$$X = xA^{-1}, \qquad Y = A^{-1}y,$$

which leaves the scalar product $X \cdot Y = x \cdot y$ invariant. While the first of the relations (2.6) is only another way of saying that when $F(x)$ is the Hölder function (1.2), the relations (2.2)–(2.4) reduce to "Hölder's inequality" together with its converses.[15]

### 3. A transformation of the same type as that of poles and polars

Given any differentiable function $\Phi(x)$ of the vector $x$, we write

$$\frac{\partial \Phi}{\partial x} = \left( \frac{\partial \Phi}{\partial x_1}, \cdots, \frac{\partial \Phi}{\partial x_n} \right)$$

for the *gradient* of $\Phi(x)$.

Let us suppose that $\Phi(x)$ is the function of distance of a certain convex body containing the origin. The transformation

$$y = \{\Phi(x)\}^\lambda \cdot \frac{\partial \Phi}{\partial x} \tag{3.1}$$

may be regarded as generalizing that of poles and polars, since it associates with any $x_0$ the coefficient $y_0$ of a certain plane (hyperplane) $x \cdot y_0 = 1$, where, if $x_0$ lies on the boundary $\Phi(x) = 1$ of our convex body, $xy_0 = 1$ is the corresponding tangent plane (hyperplane).

This being so, the relation $G(y) \leqq 1$ may be written

$$\Phi(x) \left\{ G\left( \frac{\partial \Phi}{\partial x} \right) \right\}^{1/\lambda} \leqq 1,$$

and in this form the left-hand side is homogeneous of the first order.

---

[14] The relation (2.5) is valid when these two functions are quite arbitrary functions of distance of convex bodies containing the origin, and $M_{\alpha\beta}$ is defined by (1.1).

[15] Hardy, Littlewood and Polya, loc. cit., p. 26, theorems 14 and 15.

Incidentally we see that the inequality of Minkowski-Mahler generalizes that of Hölder. Other generalizations are studied in Hardy, Littlewood and Polya's book, pp. 81–83. But that of Minkowski-Mahler is perhaps the simplest and most elegant, especially as it links up the inequality with a subject apparently far removed from it, namely with the geometry of poles and polars.

Writing $k$ for $1/\lambda$, we consider the function

$$f(x) = \Phi(x)\left\{G\left(\frac{\partial\Phi}{\partial x}\right)\right\}^k. \tag{3.2}$$

This function may be regarded as a *transform* of the function $F(x)$ when $F(x)$ and $G(y)$ are polar functions. It may be observed that, when $k = 1$, and when $\Phi(x)$ is chosen to be the function of distance of the unit sphere, the transform $f(x)$ reduces to $G(x)$.

Suppose now that, together with $\Phi(x)$, $F(x)$ and the transform $f(x)$, we consider two further functions of distance of convex bodies containing the origin, $\Phi^*(x)$, $F^*(x)$, and that we form the corresponding transform

$$f^*(x) = \Phi^*(x)\left\{G^*\left(\frac{\partial\Phi^*}{\partial x}\right)\right\}^k. \tag{3.3}$$

*We assert that the following simple inequality holds*:

$$\left\{\operatorname*{Max}_x \frac{f^*(x)}{f(x)}\right\}\left\{\operatorname*{Max}_x \frac{F^*(x)}{F(x)}\right\}^k \geqq \left\{\operatorname*{Max}_x \frac{\Phi^*(x)}{\Phi(x)}\right\}^{1+k}. \tag{3.4}$$

In fact, denoting by $M$ the maximum of $\Phi^*(x)/\Phi(x)$, we have, at a point $x_0$ for which this maximum is attained

$$\left[\frac{\partial\Phi^*}{\partial x}\right]_{x=x_0} = M\left[\frac{\partial\Phi}{\partial x}\right]_{x=x_0} = My_0, \quad \text{say.}$$

Consequently, if we remember that, exactly as in (2.5),[16]

$$\operatorname*{Max}_x \frac{F^*(x)}{F(x)} = \operatorname*{Max}_y \frac{G(y)}{G^*(y)},$$

we find that the left-hand side of (3.4) is not less than the number

$$\frac{f^*(x_0)}{f(x_0)}\left\{\frac{G(y_0)}{G^*(y_0)}\right\}^k = M^{1+k}.$$

This completes the proof of the inequality (3.4).

## 4. Elementary lemmas concerning the function $S_r(x)$

We observe that the function $S_r(x)$, defined in (1.4), has the property that, for $r > 1$,

$$\frac{1}{r}\left|\frac{\partial S_r}{\partial x_{2h-1}} + i\frac{\partial S_r}{\partial x_{2h}}\right| = |x_{2h-1} + ix_{2h}|^{r-2}\cdot\frac{1}{2}\left|\frac{\partial S_2}{\partial x_{2h-1}} + i\frac{\partial S_2}{\partial x_{2h}}\right|$$

$$= |x_{2h-1} + ix_{2h}|^{r-1}.$$

Hence, *for* $s > 0$ *and* $t > 0$,

$$S_t\left(\frac{1}{s+1}\frac{\partial S_{s+1}}{\partial x}\right) = S_{ts}(x). \tag{4.1}$$

[16] Cf. footnote fourteen.

Another property of the sums $S_r(x)$ that we shall require, is that *if* $0 \leqq \alpha \leqq 1$, $r > 0, t > 0$ *and* $r\alpha + t(1 - \alpha) = s$, *then*[17]

$$S_s(x) \leqq \{S_r(x)\}^{\alpha} \cdot \{S_t(x)\}^{1-\alpha}. \tag{4.2}$$

It is convenient to express (4.2) a little differently as follows:

(4.3) *Suppose that* $r > 0, t > 0, \lambda + \mu = \dfrac{1}{s} > 0$, *and that the function*

$$\varphi(x) = \{S_r(x)\}^{\lambda}\{S_t(x)\}^{\mu}$$

*is homogeneous of degree* 1 *in* $x$. *Then*

$$\varphi(x) \geqq \{S_s(x)\}^{1/s} \quad \textit{if } \lambda, \mu \textit{ are both positive while} \tag{4.4}$$

$$\varphi(x) \leqq \{S_s(x)\}^{1/s} \quad \textit{if } \lambda, \mu \textit{ are of opposite signs.} \tag{4.5}$$

Suppose first that $\lambda \geqq 0$, $\mu \geqq 0$, and write $\alpha = \lambda s$, so that $\mu s = 1 - \alpha$ and $0 \leqq \alpha \leqq 1$. Then (4.4) is equivalent to (4.2), which is satisfied since

$$r\alpha + t(1 - \alpha) = s(r\lambda + t\mu) = s$$

on account of the relation $r\lambda + t\mu = 1$ which follows from the fact that $\varphi(x)$ is homogeneous of degree 1.

Suppose now that $\lambda$ and $\mu$ have opposite signs, and without loss of generality, let $\lambda \leqq 0 < \mu$. In this case (4.5) may be written

$$\{S_t(x)\}^{1/t} \leqq \{S_s(x)\}^{1/(s\mu t)} \qquad S_r(x)^{-\lambda/(\mu t)} \tag{4.6}$$

and is a consequence of (4.4) since the exponents are now positive on the right, their sum being

$$\frac{1}{s\mu t} - \frac{\lambda}{\mu t} = \frac{1}{\mu t}\left(\frac{1}{s} - \lambda\right) = \frac{1}{\mu t} \cdot \mu = \frac{1}{t},$$

and since the right-hand side of (4.6) is homogeneous in $x$ of degree

$$s \cdot \frac{1}{s\mu t} + r\,\frac{-\lambda}{\mu t} = \frac{1}{\mu t}(1 - r\lambda) = \frac{1}{\mu t} \cdot \mu t = 1.$$

This completes the proof.

## 5. Transforms of Hölder functions

Suppose that $\Phi(x)$ and $F(x)$ are the two Hölder functions $F_\alpha(x)$ and $F_{\alpha_1}(x)$. The transform $f(x)$ exists, if $0 < \alpha < 1$, since $F_\alpha(x)$ is differentiable, and we find, by (4.1),

$$\begin{aligned} f(x) &= \{F_\alpha(x)\}^{1+k-k/\alpha} \cdot \left\{S_{1/(1-\alpha_1)}\left(\frac{1}{\alpha}\,\frac{\partial S_{1/\alpha}}{\partial x}\right)\right\}^{k(1-\alpha_1)} \\ &= \{S_r(x)\}^{(1+k)\alpha-k}\{S_t(x)\}^{k-\alpha_1 k}, \end{aligned} \tag{5.1}$$

where $r = 1/\alpha$ and $t = (\alpha^{-1} - 1)/(1 - \alpha_1)$.

[17] Hardy, Littlewood and Polya, loc. cit., p. 27 (6 lines from the bottom).

Writing $\alpha_2 = \alpha + k(\alpha - \alpha_1)$ for the sum of the exponents of $S_r(x)$ and $S_i'(x)$ on the right of (5.1), we deduce at once from (4.3) the following result.

(5.2) *Suppose that* $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$, $k > 0$, *and* $\alpha_2 = \alpha + k(\alpha - \alpha_1)$.[18] *Let* $\Phi(x) = F_\alpha(x)$ *and* $F(x) = F_{\alpha_1}(x)$, *and let* $f(x)$ *be their transform defined in* (3.2). *Then*

$$f(x) \geqq F_{\alpha_2}(x) \quad \text{if} \quad \alpha \geqq \frac{k}{1+k}, \tag{5.3}$$

*while*

$$f(x) \leqq F_{\alpha_2}(x) \quad \text{if} \quad \alpha \leqq \frac{k}{1+k}. \tag{5.4}$$

Exactly the same property as is expressed by (5.2), for the system of functions $F_\alpha(x)$ $(0 < \alpha < 1)$, holds also for the system of functions $F_\beta^*(x)$ $(0 < \beta < 1)$, and may be stated as follows:

(5.5) *Suppose that* $0 < \beta_1 < 1$, $0 < \beta_2 < 1$, $k > 0$ *and* $\beta_2 = \beta + k(\beta - \beta_1)$. *Let* $\Phi^*(x) = F_\beta^*(x)$ *and* $F^*(x) = F_{\beta_1}^*(x)$, *and let* $f^*(x)$ *be their transform defined in* (3.3). *Then*

$$f^*(x) \geqq F_{\beta_2}^*(x) \quad \text{if} \quad \beta \geqq \frac{k}{1+k}, \tag{5.6}$$

*while*

$$f^*(x) \leqq F_{\beta_2}^*(x) \quad \text{if} \quad \beta \leqq \frac{k}{1+k}. \tag{5.7}$$

To deduce (5.5) from (5.2) it is sufficient to remark that *if we write* $\Phi^*(x) = \Phi(x \cdot A)$ *and* $F^*(x) = F(x \cdot A)$ *then* $f^*(x) = f(x \cdot A)$ *where* $f(x)$ *is defined by* (3.2). This is so, since the polar functions of $F^*(x)$ and $F(x)$ fulfil the relation $G^*(y) = G(A^{-1}y)$ and therefore, writing $X$ for $xA$,

$$G^*\left(\frac{\partial \Phi^*}{\partial x}\right) = G^*\left(A\,\frac{\partial \Phi(X)}{\partial X}\right) = G\left(A^{-1}A\,\frac{\partial \Phi(X)}{\partial X}\right)$$
$$= G\left(\frac{\partial \Phi(X)}{\partial X}\right).$$

## 6. Proof of Marcel Riesz's theorem

Let us now write

$$t = \frac{k}{k+1}, \qquad m = \operatorname*{Max}_x \frac{f^*(x)}{f(x)}$$

[18] These relations evidently imply $0 < \alpha < 1$ since $\alpha$ may be written $(k\alpha_1 + \alpha_2)/(k+1)$ as a mean of $\alpha_1$ and $\alpha_2$.

so that $k > 0$ becomes $0 < t < 1$, and the relations between $\alpha_1$, $\alpha_2$, and $\alpha$, and between $\beta_1$, $\beta_2$, and $\beta$ become identical with (1.8).

Choosing $\Phi$, $F$, $\Phi^*$, $F^*$ as in (5.2) and (5.5) it is clear on the one hand that (3.4) gives

$$(M_{\alpha_1\beta_1})^t m^{1-t} \geqq M_{\alpha\beta}, \tag{6.1}$$

while on the other hand, from (5.3) and (5.7),

$$m \leqq M_{\alpha_2\beta_2} \quad \text{if} \quad \alpha \geqq t \geqq \beta. \tag{6.2}$$

Hence to establish (1.6) it is sufficient to show that there exists at least one value of $t$ such that $\alpha \geqq t \geqq \beta$ where $\alpha$ and $\beta$ are the linear functions of $t$ given by (1.8) and where $0 < t < 1$. Now for *every* $t$ in $0 < t < 1$, we have $0 < \beta < \alpha < 1$. If therefore we choose $t = \alpha = \alpha_2/[\alpha_2+(1 - \alpha_1)]$, the conditions are satisfied.

This completes the proof of (1.6) and so of (1.5).

TRINITY COLLEGE,
CAMBRIDGE, ENGLAND.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# LINEAR TOPOLOGICAL GROUPS

BY E. W. PAXSON

(Received November 3, 1938)

We wish to demonstrate the following

THEOREM. *Every Abelian, convex, connected, and sequentially complete topological (Hausdorff) group, which possesses no elements of finite order, is a pseudo-normed linear topological space.*

A group so conditioned may be called *linear topological.* For the notion of pseudo-norm see [1] p. 18.

1. Let $\mathfrak{G}$ denote an abstract set of elements called points subjected to a Hausdorff neighborhood topology ([2] pp. 228–9) and supporting a group composed additively with identity written 0. Following [3] we formulate continuity of the group operations in the following convenient fashion (neighborhoods of $a \in \mathfrak{G}$ being written $U_a$, $V_a$, $W_a$ etc.):

S1. *For every $U_{a+b}$ there exist $U_a$ and $U_b$ such that*

$$U_a + U_b \subset U_{a+b}.$$ [1]

S2. *For every $U_0$ there exists $V_0$ such that*

$$-V_0 \subset U_0.$$

We suppose further that $\mathfrak{G}$ is connected. If $\mathfrak{G}$ satisfies also

S3. *For every $U_0$ and each positive integer $n$*

$$U_0^n \subset nU_0,$$

*then $\mathfrak{G}$ is said to be convex.* Under convexity it is clear that $U_0^n = nU_0$.

LEMMA 1. *For every $U_0$ there exists $W_0$ such that $\pm W_0 \subset U_0$.*

For we have $-V_0 \subset U_0$, and a $W_0 \subset V_0 \cap U_0$. Then $-W_0 \subset -V_0$ etc.

LEMMA 2. *The topologies $\{U_a\}$, $\{U_0 + a\}$ and $\{a + U_0\}$ are equivalent.*

By [3] (Lemma 1) each $a \in \mathfrak{G}$ and each $U_0$ determine $U_a$ such that $U_a \subset a + U_0$ and $U_a \subset U_0 + a$. Also for $a = a$ and $b = -a$ we have for any $U_a$ by the same lemma $U_{a-a} = U_0$ such that $U_0 \subset U_a - a$, $(U_0 + a \subset U_a)$ and $U_0 \subset -a + U_0$, $(a + U_0 \subset U_a)$.

This uniformization permits us to topologize $\mathfrak{G}$ entirely through neighborhoods of 0, now to be written $U$, $V$, $W$ etc.

LEMMA 3. *The operations $a + b$ and $-a$ are continuous.*

We have by S1 for any $U$, $V_1$ *and* $V_2$ such that $V_1 + V_2 \subset U$. Also $W \subset V_1 \cap V_2$ and hence $W + W \subset U$. Continuity of $+$ is immediate. Hence continuity of the inverse need be proved only at 0 and S2 makes this clear.

[1] $A + B$ means the set of all $a + b$, $a \in A$, $b \in B$. $nA$ ($n$ a positive integer) means the set of all $na = a + a + \cdots + a$ ($n$ summands) with $a \in A$. $A^n$ means $A + A + \cdots + A$ ($n$ summands).

In the sequel $\mathfrak{G}$ shall be taken Abelian.

DEFINITION 1. *A set $S \subset \mathfrak{G}$ is said to be bounded if for every $U$ there exists a positive integer $n$ such that $S \subset U^n$.*

LEMMA 4. *If $\mathfrak{G}$ is connected then every $(a) \subset \mathfrak{G}$ is bounded.*

For by [3] (Theorem 3) a connected group is covered by all finite iterations of any neighborhood of the identity.

THEOREM 1. *$\mathfrak{G}$ is a regular topological space.*

We have only to show that for every $U$ there is determined $V$ such that $\bar{V} \subset U$, where the bar denotes closed hull. As in Lemma 3 $W + W \subset U$. Choose $V$ such that $\pm V \subset W$. Take $p \in \bar{V}$. Then there exists $q \in V$ such that $q \in p + V$. Hence $-p \in -q + V$ or $p \in q - V \subset V - V \subset W + W \subset U$, whence $\bar{V} \subset U$.

LEMMA 5. *The sets $U + V$ and $U^n$ are open. If $\mathfrak{G}$ is convex $\bar{U}^n = \overline{U^n} = \overline{nU} = n\bar{U}$.*

These relations follow without difficulty.

**2.** In the presence of convexity we can introduce formally in $\mathfrak{G}$ a notion of rational linearity relative to any designated neighborhood of the identity. That is, the multiplier domain shall consist (for the present) only of real rationals.

DEFINITION 2. *$(1/n)\,p = q$ means $p = nq$ where $n$ is a positive integer. Thus $mnq = mp$ is written $mq = x = (m/n)p$.*

THEOREM 2. *The space $\mathfrak{G}$ is closed under such multiplication.*

Take $p \in U$. Let $m$, $n$ be any positive integers. By convexity there exists $q \in U$ such that $p = nq$ since $U \subset U^n = nU$. Thus $(1/n)p = q$ and $(m/n)p = mq$, so that $(m/n)p$ is well defined. This may be extended to any $p \in \mathfrak{G}$. For by [3] (Theorem 3 and Lemma 6) $p = Nq$ where $q \in U$ and $N$ is a positive integer. Then $(mN/n)q$ exists as above and so also $(m/n)p$. To continue this to the negative rationals we observe that since $\mathfrak{G}$ is connected $\mathfrak{G} = \lim_{N\to\infty} N \cdot U$. Hence for any $-p \in \mathfrak{G}$, $(m/n)(-p)$ is well defined. This may be written $(-m/n)p$ to complete the argument.

THEOREM 3. *If $p \in \mathfrak{G}$ and $(m/n)$ is an arbitrary rational number, the element $q = (m/n)p$ is independent of $U$ (is unique) if and only if $\mathfrak{G}$ has no elements except the identity of finite order.*

Let $q_U = (m/n)p$ relative to $U$ and $q_V = (m/n)p$ relative to $V$. Then $nq_U = mp = nq_V$. Thus $nq_U = nq_V$. This implies $q_U = q_V$ if and only if $q_U - q_V$ is not of finite order $n$.

Notice that $(1/n)\,0$ is not uniquely 0 in groups with non-0 elements of finite order, as in, for example, the group of all rotations of a triangle where elements of all orders exist. Hence in what follows we take $(m/n)p$ unique by stipulating that the group be of the type of the theorem.

THEOREM 4. *For each $U$ there exists $W$ such that $\beta W \subset U$ for $\beta$ rational and $-1 \leqq \beta \leqq 1$.*

Choose $W$ with $\pm W \subset U$. By convexity $\beta^+ W \subset W$, $\beta^+$ rational and $0 \leqq \beta^+$

$\leqq 1$. For if for some $\beta^+$, say $\gamma$, $\gamma W \not\subset W$, we have ($\gamma = (m/n)$, $m < n$) $mW \not\subset nW$, $W^m \not\subset W^n$ which is a contradiction.

THEOREM 5. *The product $(m/n)p$ is continuous in $p$ and rationally continuous in $(m/n)$ (in an obvious sense).*

Since addition is continuous we may discuss the situation at the identity. Fix $m/n$ and take $p = 0$. Let $N$ be the smallest integer such that $2^N > m/n$. Choosing $V_1, V_2, \cdots$ as in Lemma 3 we have, using convexity, for any $U$, $V_N$ such that $2^N V_N \subset U$. Then $p \in V_n$ implies $(m/n)p \in U$ since $(m/n)V_n = \beta^+ \cdot 2^N V_n \subset 2^N V_N$ by Theorem 4 with $0 \leqq \beta^+ \leqq 1$; $m/n$ being taken with no loss of generality positive. Next fix $p$ and choose $(m/n) = 0$. By Lemma 4 there exists $N$ such that for any $W$, $p \in W^N = N \cdot W$. By Theorem 4 take this $W$ such that $\beta W \subset U$ for an arbitrary $U$ and $-1 \leqq \beta \leqq +1$, $\beta$ rational. Then choosing $\delta = (1/N)$ we have $|\alpha| < (1/N)$, $\alpha$ rational, implying $\alpha p \in U$.

THEOREM 6. *$\mathfrak{G}$ is rational linear under the group sum and the multiplication above.*

We need be concerned only with multiplication and, in fact, with multiplication by positive rationals of the form $1/n$. Now $(1/n)(f+g) = p$ or $f+g = np$. Also $n(\overline{1/n}f + \overline{1/n}g) = f + g = np$ or $(1/n)f + (1/n)g = p$. Consider next $\overline{1/n}(\overline{1/s}f)$. Then $f = sp$ and $p = nq$. Thus $f = nsq$ or $\overline{1/ns}f = q$. But $\overline{1/s}f = p = nq$. Hence $\overline{1/n}(\overline{1/s}f) = q$. Lastly take $(\overline{1/n} + \overline{1/s})f = q$. Now $\overline{n+s}f = nf + sf = nsq$ and $q = \overline{1/ns}(nf + sf) = \overline{1/s}f + \overline{1/n}f$ by the properties above.

THEOREM 7. *For all rationals $\alpha$, $\beta$, $0 \leqq \alpha < \beta$ (or $\beta < \alpha \leqq 0$) and for any $U$, $\overline{\alpha U} \subset \beta U$.*

Choose $V$ so that $(\pm V)^n \subset U$. Take $p \in \bar{U}$ ($np \in n\bar{U}$). Then there exists $q \in U$ so that $q \in p + V$ or $nq \in np + nV$ or $np \in nq - nV$. Thus $np \in nU + U = \overline{n+1}U$ by convexity. Hence $n\bar{U} \subset \overline{n+1}U$. Next it follows that $\alpha U + (1-\alpha)U = U$ for $\alpha = m/n (n \geqq m \geqq 0)$. For $mU + (n-m)U = U^n = nU$ by convexity and the result follows from the rational linearity. Since $0 \in U$ we have from the above $\alpha U \subset U$ for every rational $\alpha$, $0 \leqq \alpha \leqq 1$. These remarks apply also to $\bar{U}$. Finally, choosing $n$ large enough so that $(\beta n/\overline{n+1}) > \alpha$ we have

$$\alpha\bar{U} \subset (\beta n/\overline{n+1})\bar{U} \subset \beta U.$$

3. Theorem 7 permits us to induce in $\mathfrak{G}$ a pseudo-norm.

THEOREM 8. *There exists a continuous function (written $\| p \|_U^+$ following* [1] p 18) *that is on $\bar{U}$ to* [0, 1] *and is such that $\| 0 \|_U^+ = 0$ and $\| p \|_U^+ = 1$ for $p$ the frontier of $\bar{U}$.*

By Theorem 7 we have for each $n$ a sequence $\{\overline{m/2^n}U\}$ where $m = 0, 1, \cdots, 2^n$ such that

$$\overline{(m'/2^n)}\bar{U} \subset (m''/2^n)U \qquad (m' < m'').$$

By the same theorem for any $m < 2^n$ there exists $(\overline{m+\frac{1}{2}}/2^n)U$ such that

$$\overline{(m/2^n)}\bar{U} \subset \overline{(m+\tfrac{1}{2}/2^n)}U \subset (\overline{m+1}/2^n)U.$$

Thus for all dyadic rationals a sequence $\{\overline{m/2^n U}\}$ with the closure inclusion property is defined inductively (tacit appeal being made to the Zermelo axiom). Now the sets

$$A = \prod_{\alpha>0} \alpha\bar{U} \quad \text{and} \quad B = \bar{U} \ominus \prod_{\beta<1} \beta U$$

($\alpha$, $\beta$ rationals) are closed sets, the first as the intersection of closed sets[2] and the second as the frontier of $\bar{U}$ (remembering regularity). Now all details of the celebrated Urysohn Lemma (as in [4] p. 74) follow for $\bar{U}$ (considered as a relative space). Thus the existence of a continuous function is assured with value 0 over $A$ and 1 over $B$. It is monotonic throughout $\bar{U}$ in the sense that

$$\| p \|_U^+ = \text{g.l.b.}_{p \in \alpha U}\{\alpha\} \qquad \text{(rational } \alpha\text{)}$$

referring again to Theorem 7. That is, this Urysohnian construction is equivalent to the attitude of v. Neumann ([1], p 18).

THEOREM 9. *There exists a continuous function* $\| p \|_U$ *defined throughout* $\mathfrak{G}$ *with the properties*: a) $\| p \|_U \geqq 0$, $= 0$ *if and only if* $p \in A$ *(as above)*; b) $\| \alpha p \|_U = | \alpha | \cdot \| p \|_U$ *($\alpha$ rational)*; c) $\| p + q \|_U \leqq \| p \|_U + \| q \|_U$.

For any $q \in \mathfrak{G}$ by convexity and connectedness we have $p \in U$ such that $q = np$ for some positive integer $n$. Define $\| q \|_U^+ = n \cdot \| p \|_U^+$. The continuity is evident. In a fashion analogous to the process of Theorem 7 construct $\| p \|_U^- = \text{g.l.b.}_{p \in -\alpha U}\{\alpha\}$ ($\alpha$ positive rational). Define finally

$$\| p \|_U = \max \{ \| p \|_U^+ , \| p \|_U^- \}.$$

As the maximum of two continuous functions $\| p \|_U$ is continuous. It is defined throughout $\mathfrak{G}$. It satisfies

$$\| p \|_U = \| -p \|_U .$$

From the definitions a) and b) now becomes obvious. It remains to prove the triangular inequality. To this end choose positive rational numbers $\alpha_p^\pm$ and $\alpha_q^\pm$ such that for an arbitrary $\delta > 0$,

$$\| p \|_U^\pm + \delta < \alpha_p^\pm < \| p \|_U + 2\delta, \qquad \| q \|_U^\pm + \delta < \alpha_q^\pm < \| q \|_U + 2\delta.$$

Then

$$p \in \pm \alpha_p^\pm U, \qquad q \in \pm \alpha_q^\pm U, \qquad p + q \in \pm (\alpha_p^\pm + \alpha_q^\pm) U$$

by convexity. For from $\alpha U + (1 - \alpha)U = U$ we have

$$(\beta/\overline{\beta + \gamma})U + (\gamma/\overline{\beta + \gamma})U = U.$$

Then

$$\| p + q \|_U^\pm \leqq \alpha_p^\pm + \alpha_q^\pm < \| p \|_U + \| q \|_U + 4\delta.$$

But $\delta$ is arbitrary, giving the result.

We remark particularly on the relativity of this norm concept. One should compare [1] p. 18, to which this discussion is parallel. It is to be noted that

[2] Cf. Hilbert space weakly topologised as in [1] p. 15 where the notion of orthogonality makes $(+0)U = A$ contain elements other than 0.

$p \in U$ does not necessarily imply that $\| p \|_U < 1$. For then we would always have $p \in U$ implying $-p \in U$. That this is not necessarily true is seen from the example of the plane with neighborhoods taken as proper ellipses with one focus at the origin. That is, qualitatively speaking, the pseudo-unit-sphere is uniformly full.

THEOREM 10. *If $\mathfrak{G}$ is sequentially complete a meaning can be assigned to $\beta \cdot p$ where $\beta$ is irrational and $p \in \mathfrak{G}$ such that $\mathfrak{G}$ is closed under such (and rational) multiplication, such that $\beta \cdot p$ is continuous in the pair, and such that under it $\mathfrak{G}$ is completely linear.*

We show first that if $\{\alpha_m\}$ is a sequence of rationals with irrational $\beta$ as limit then for any $p$ the sequence $\{\alpha_m p\}$ is fundamental. Let $U$ be arbitrary. Then by the rational continuity of the product $\alpha \cdot p$ there exists $\delta > 0$ such that $|\alpha| < \delta$, $\alpha$ rational, implies $\alpha p \in U$. Since $\alpha_m \to \beta$, $\{\alpha_m\}$ is a real fundamental sequence and hence for a chosen $\delta$ there exists $N$ such that $n, m > N$ imply $|\alpha_n - \alpha_m| < \delta$ where $\alpha_n - \alpha_m$ is rational. Thus $(\alpha_n - \alpha_m)p = \alpha_n p - \alpha_m p \in U$ for $n, m > N(U)$. Assuming sequential completeness $\alpha_m p \to q$ which we shall write $\beta \cdot p$. This is unique.

We next show that $U$ determines $V$ so that $\beta V \subset U$ for all $\beta$, $-1 \leqq \beta \leqq 1$. Choose $W$ as in Theorem 4. Select $V$ through regularity so that $\bar{V} \subset W$. Then $\alpha \bar{V} \subset \alpha W^* \subset U$ ($\alpha$ rational, $-1 \leqq \alpha \leqq 1$). Let $p \in V$ and take $\alpha_m \to \gamma$, $\alpha_m$ rational, $\gamma$ irrational, $-1 \leqq \alpha_m, \gamma \leqq 1$. Then $\{\alpha_m p\}$ is a sequence from $\alpha V$ with $\gamma \cdot p$ as limit. Thus $\gamma p \in \bar{V}$. Hence $\beta V \subset U$ for all $\beta$, $-1 \leqq \beta \leqq 1$. Now exactly as in Theorem 5 we prove that $\beta \cdot p$ is continuous in $\beta$ (in an ordinary sense. Continuity of $\beta \cdot p$ in the pair is also immediate.

It is easy to see that $\beta \cdot p$ has the requisite properties of the product in a linear space. One uses sequences of rationals and continuity. We notice also that $\| \beta p \|_U = |\beta| \cdot \| p \|_U$ for all $\beta$. For $\| \alpha_n p \|_U = |\alpha_n| \cdot \| p \|_U$ and the result follows from the continuity of the pseudo-norm.

The main Theorem of the paper may now be considered proved. It is further clear that the set of pseudo-spheres $\| p - p_0 \| < \delta$ is a complete neighborhood system for $\mathfrak{G}$.

4. A word with regard to the coalescence of these ideas with the customary ones in more common situations is to the point. Let now $\mathfrak{G}$ be a metric group with neighborhoods $U$ taken as open spheres about 0. Then the pseudo-spheres $\| p \|_V < 1$ clearly coincide in extent with the spheres $\rho(0, p) < \delta$ where $\delta > 0$ determines $V$ (the base neighborhood $U$ being $\rho(0, p) < 1$ and of course $\prod_{\alpha > 0} \alpha U = (0)$). But we can only say that the pseudo-norm topology is equivalent to the pre-existent metric topology. That is $\| p \|_U$ and $\rho(0, p)$ are not necessarily equal for all $p \in \mathfrak{G}$. For consider the space $E_\omega$ (Fréchet) of all sequences $x \equiv (x_1, x_2, \cdots, x_n, \cdots)$ under the metric

$$\rho(x, y) = \sum_{n=1}^{\infty} \frac{1}{(n-1)!} \frac{|x_n - y_n|}{1 + |x_n - y_n|}.$$

$E_\omega$ then has placewise convergence, is bounded, but not compact. Choose $U$ as the sphere of radius 1 and construct $\| \cdots \|_U$. Then $\rho(0, x) = 1$ is equivalent to $\| x \|_U = 1$ but for all other non-zero elements $y$, $\rho(0, y) \neq \| y \|_U$ because the pseudo-norm has the homogeneity property and the Fréchet metric has not.

This last example shows that in linear metric spaces which we do not know how to norm the pseudo-norm becomes a true, albeit non-effective, norm (in the sense that it is not explicitly exhibited) topologically equivalent to the metric. So in the space of all real uniform functions on [0, 1] it is possible to introduce effectively a metric and hence construct a norm.[3]

In the case of a complete normed vector space we have true coincidence in regard to linearity and norm. In what follows the subscript $C$ will refer to entities constructed on the module of the space according to the above text. First $(1/n)p = (\overline{1/n}p)_C$ since $(\overline{1/n}\cdot p)_C$ is found by $p = nq$ from $\| p \| = n \| q \|$ ($p \in U$ implying $\| p \| < 1$). Similarly for $\overline{m/n}p = (\overline{m/n}p)_C$. Again, limits of sequences being unique under the separation axiom, we have $\alpha p = (\alpha p)_C$ ($\alpha$ irrational) since the same approximating rational sequences are used. Finally $\| p \| = (\| p \|)_C$. For certainly $\| q \| = 1$ implies $(\| q \|)_C = 1$. Take $q = \| p \|^{-1} \cdot p$. Then $\| q \| = 1$, so that $\| p \| = \| p \| \cdot \| q \| = \| p \|$ and $(\| p \|)_C = \| p \| (\| q \|)_C = \| p \|$.

WAYNE UNIVERSITY,
DETROIT, MICHIGAN.

## BIBLIOGRAPHY

[1] J. v. NEUMANN, *On complete topological spaces*, Trans. A. M. S. 37 (1935), pp. 1-20.
[2] F. HAUSDORFF, *Mengenlehre*, Berlin, 1927.
[3] F. LEJA, *Sur la notion du groupe topologique*, Fund. Math. 10.
[4] ALEXANDROFF AND HOPF, *Topologie* 1, Berlin, 1935.

[3] We wish to discuss this at length elsewhere.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# DIMENSIONALITY IN REDUCIBLE GEOMETRIES

BY ISRAEL HALPERIN[1]

(Received August 17, 1938)

## 1. Introduction

The dimensionality theory of projective and continuous geometries discovered by J. v. Neumann ([1], [2], [3]) depends in an essential way on the irreducibility of the geometry. The purpose of the present paper is to extend the dimensionality theory to the case of a reducible geometry which is however irreducible under a suitable group of automorphisms of the geometry. This will be done with the help of a general theorem on the superposition of decompositions.[2] In the last § a process of integration will be defined by means of which a general class of such reducible geometries will be constructed.

## 2. Axioms and notation

We shall consider a geometry which may be reducible or irreducible, that is, a system $L$ of elements $a, b, c, \cdots$ which is partially ordered by a relation $<$, and is complemented, modular, complete, and continuous—in other words, it satisfies the Axioms I, II, III, IV, V but not necessarily the Axiom VI (irreducibility) of von Neumann [1], [2]. The notation of [1], [2] will be used and those parts of [2] which depend only on Axioms I–V will be assumed: in particular, the theory of independence,[3] the theory of perspective mappings and the transitivity of perspectivity.[4] Also, $\oplus$ will sometimes be used in place of $+$ when the summands are independent, and if $a \geqq b$ then $[a - b]$ will denote some (fixed) element such that $a = b \oplus [a - b]$. The same symbols $+, \sum, \prod, 0, 1$, will be used in different geometries or systems, but there should be no confusion.

## 3. Superposition of decompositions

We require the following lemmas.[5]

[1] This paper was begun while the author was Sterling Research Fellow at Yale University.

[2] The desire to find such a theorem arose from a remark of J. v. Neumann emphasizing the failure in general geometries of the usual superposition of decompositions in Boolean algebras. The writer is also greatly indebted to Professor von Neumann for many friendly discussions and helpful suggestions.

[3] A set of elements $a_\alpha$, $\alpha \in I$, is independent if $\left(\sum_{\alpha \in J} a_\alpha\right)\left(\sum_{\alpha \in K} a_\alpha\right) = 0$ for all mutually exclusive subsets $J, K$ of $I$. Repeated application of Lemma 3.1 shows that $a_\alpha$, $\alpha \in I$, are independent if and only if every finite subset of $a_\alpha$, $\alpha \in I$ is independent.

[4] See [2], Part 1, Chapters I–V, Part III, Chapters I, II. See also [4].

[5] Lemmas 3.1–3.4 are contained implicitly, in somewhat specialized form, in [2].

LEMMA 3.1. *If* $b\sum_{\alpha \in J} c_\alpha = 0$ *for every finite subset* $J$ *of* $I$, *then* $b\sum_{\alpha \in I} c_\alpha = 0$.

PROOF. If possible, suppose $b\sum_{\alpha \in I} c_\alpha \neq 0$ and let $K$ be a subet of $I$ of least cardinal power such that $b\sum_{\alpha \in K} c_\alpha \neq 0$. From the hypothesis, $K$ cannot be finite. Hence we may assume $K$ is the set of ordinals $<\Omega$ for some limit ordinal $\Omega$ such that the set of ordinals $<\gamma$ has cardinal power less than that of $K$ for all $\gamma < \Omega$. Then $b\sum_{\alpha<\gamma} c_\alpha = 0$ for all $\gamma < \Omega$. By the continuity axiom (III), this implies

$$b \sum_{\alpha<\Omega} c_\alpha = b\Big(\sum_{\gamma<\Omega} \sum_{\alpha<\gamma} c_\alpha\Big) = \sum_{\gamma<\Omega} \Big(b \sum_{\alpha<\gamma} c_\alpha\Big) = \sum_{\gamma<\Omega} 0 = 0,$$

which contradicts the assumption on $K$. Hence $b\sum_{\alpha \in I} c_\alpha$ must $= 0$ as required.

LEMMA 3.2. *If* $a_\alpha$, $\alpha \in I$, *are independent and* $a_{\alpha,\lambda} \leqq a_\alpha$ *for all* $\alpha$, $\lambda$, *then*

$$\prod_\lambda \Big(\sum_{\alpha \in I} a_{\alpha,\lambda}\Big) = \sum_{\alpha \in I} \Big(\prod_\lambda a_{\alpha,\lambda}\Big).$$

PROOF. Since $\geqq$ is clear we may set

$$b = \Big[\prod_\lambda \Big(\sum_{\alpha \in I} a_{\alpha,\lambda}\Big) - \sum_{\alpha \in I} \Big(\prod_\lambda a_{\alpha,\lambda}\Big)\Big].$$

We now show that for every finite set $\alpha_1, \cdots, \alpha_N$

$$\prod_\lambda \Big(\sum_{r=1}^N a_{\alpha_r,\lambda}\Big) = \sum_{r=1}^N \Big(\prod_\lambda a_{\alpha_r,\lambda}\Big). \tag{1}$$

By Theorem 1.2 of [2], Part I, or Lemma 2.8 of [4] we have

$$(a_{\alpha_1,\lambda_1} + a_{\alpha_2,\lambda_1})(a_{\alpha_1,\lambda_2} + a_{\alpha_2,\lambda_2}) = a_{\alpha_1,\lambda_1} a_{\alpha_1,\lambda_2} + a_{\alpha_2,\lambda_1} a_{\alpha_2,\lambda_2}.$$

Repeated application of this result and induction on $M$ gives

$$\prod_{r=1}^M (a_{\alpha_1,\lambda_r} + a_{\alpha_2,\lambda_r}) = \prod_{r=1}^M (a_{\alpha_1,\lambda_r}) + \prod_{r=1}^M (a_{\alpha_2,\lambda_r})$$

for every finite set $\lambda_1, \cdots, \lambda_M$. Hence, using the continuity axiom,

$$\begin{aligned}\prod_\lambda (a_{\alpha_1,\lambda} + a_{\alpha_2,\lambda}) &= \prod_{\text{all } M} \Big\{\prod_{r=1}^M (a_{\alpha_1,\lambda_r}) + \prod_{r=1}^M (a_{\alpha_2,\lambda_r})\Big\} \\ &= \prod_\lambda (a_{\alpha_1,\lambda}) + \prod_\lambda (a_{\alpha_2,\lambda}).^6\end{aligned}$$

Repeated applications of this result and induction on $N$ gives (1).

Now (1) applied to the two elements $a' = \sum_{r=1}^N a_{\alpha_r}$, $a'' = \sum_{\alpha \neq \alpha_r, r=1,\cdots,N} a_\alpha$ shows that

$$\begin{aligned} b \sum_{r=1}^N a_{\alpha_r} &= b \prod_\lambda \Big(\sum_{\alpha \in I} a_{\alpha,\lambda}\Big) \sum_{r=1}^N a_{\alpha_r} = b \prod_\lambda \Big(\sum_{r=1}^N a_{\alpha_r,\lambda}\Big) \\ &= b \sum_{r=1}^N \Big(\prod_\lambda a_{\alpha_r,\lambda}\Big) \leqq b \sum_{\alpha \in I} \Big(\prod_\lambda a_{\alpha,\lambda}\Big) = 0,\end{aligned}$$

---

[6] The continuity axiom implies that for a set of elements $c$, $d$, $\alpha \in I$, $c \prod_{\alpha \in I} d_\alpha = \prod_{\text{all finite } \alpha_1, \cdots, \alpha_n} (c \prod_{r=1}^M d_{\alpha_r})$.

that is, $b\sum_{r=1}^{N} a_{\alpha_r} = 0$ for every finite set $\alpha_1, \cdots, \alpha_N$. Since $b \leqq \sum_{\alpha \in I} a_\alpha$ it follows from Lemma 3.1 that $b = 0$. This is equivalent to the statement of the present lemma.

LEMMA 3.3. *If decompositions $a_\alpha = a_{\alpha+1} \oplus a'_\alpha$ are defined for all $0 \leqq \alpha <$ some ordinal $\Omega$ and $a_\alpha = \prod_{\beta<\alpha} a_\beta$ for all limit ordinals $\alpha \leqq \Omega$, then*

$$a_0 = a_\Omega \oplus \sum_{\alpha<\Omega} \oplus a'_\alpha. \tag{2}$$

PROOF. The proof is by transfinite induction. (2) holds by assumption if $\Omega = 1$. Now suppose that (2) has been established for all $\gamma < \Omega$. If $\Omega$ has a predecessor, $\Omega = \gamma + 1$, then

$$a_0 = a_\gamma \oplus \sum_{\alpha<\gamma} \oplus a'_\alpha, \qquad a_\gamma = a_{\gamma+1} \oplus a'_\gamma$$

imply

$$a_0 = a_{\gamma+1} \oplus a'_\gamma \oplus \sum_{\alpha<\gamma} \oplus a'_\alpha = a_\Omega \oplus \sum_{\alpha<\Omega} \oplus a'_\alpha,$$

and (2) holds for $\Omega$. If $\Omega$ is a limit ordinal, then $a'_\alpha$, $\alpha < \Omega$, are independent and

$$a_\Omega\Big(\sum_{\alpha<\Omega} a'_\alpha\Big) = a_\Omega\Big(\sum_{\gamma<\Omega}\sum_{\alpha<\gamma} a'_\alpha\Big) = \sum_{\gamma<\Omega}\Big(a_\Omega \sum_{\alpha<\gamma} a'_\alpha\Big)$$
$$= \sum_{\gamma<\Omega}\Big(a_\Omega a_\gamma \sum_{\alpha<\gamma} a'_\alpha\Big) = \sum_{\gamma<\Omega} 0 = 0,$$

implying that $a_\Omega$, $a'_\alpha$, $\alpha < \Omega$, are independent. Furthermore,

$$a_0 = \sum_{\gamma<\Omega}\Big(a_\gamma \oplus \sum_{\alpha<\gamma} \oplus a'_\alpha\Big) \geqq \sum_{\gamma<\Omega}\Big(a_\Omega + \sum_{\alpha<\gamma} a'_\alpha\Big) = a_\Omega \oplus \sum_{\alpha<\Omega} \oplus a'_\alpha,$$

and

$$a_0 = \prod_{\gamma<\Omega}\Big(a_\gamma \oplus \sum_{\alpha<\gamma} \oplus a'_\alpha\Big) \leqq \prod_{\gamma<\Omega}\Big(a_\gamma + \sum_{\alpha<\Omega} \oplus a'_\alpha\Big)$$
$$= \prod_{\gamma<\Omega} a_\gamma + \sum_{\alpha<\Omega} \oplus a'_\alpha = a_\Omega \oplus \sum_{\alpha<\Omega} \oplus a'_\alpha.$$

Thus $a_0 = a_\Omega \oplus \sum_{\alpha<\Omega} \oplus a'_\alpha$ and (2) holds for $\Omega$ in this case also. By induction the lemma holds for all $\Omega$.

LEMMA 3.4. *If $a'_\alpha = [a_\alpha - (\sum_{\beta<\alpha} a_\beta)a_\alpha]$ for all $0 \leqq \alpha < \Omega$, then*

$$\sum_{\alpha<\Omega} a_\alpha = \sum_{\alpha<\Omega} \oplus a'_\alpha. \tag{3}$$

PROOF. Since $a'_0 = a_0$, (3) holds for $\Omega = 1$. Now suppose that (3) has been established for all $\gamma < \Omega$. If $\Omega$ has a predecessor $\gamma$, then

$$\sum_{\alpha<\Omega} a_\alpha = a_\gamma + \sum_{\alpha<\gamma} a_\alpha = a_\gamma + \sum_{\alpha<\gamma} \oplus a'_\alpha$$
$$= [a_\gamma - (\sum_{\alpha<\gamma} \oplus a'_\alpha)a_\gamma] \oplus \sum_{\alpha<\gamma} \oplus a'_\alpha = \sum_{\alpha<\Omega} \oplus a'_\alpha,$$

and if $\Omega$ is a limit ordinal, then

$$\sum_{\alpha<\Omega} a_\alpha = \sum_{\gamma<\Omega}\Big(\sum_{\alpha<\gamma} a_\alpha\Big) = \sum_{\gamma<\Omega}\Big(\sum_{\alpha<\gamma} \oplus a'_\alpha\Big) = \sum_{\alpha<\Omega} \oplus a'_\alpha.$$

Hence, in either case, the lemma holds for $\Omega$. By induction the lemma holds for all $\Omega$.

THEOREM 3.1. (SUPERPOSITION OF DECOMPOSITIONS). *If* $b = \sum_{\alpha<\Omega_1} a_\alpha = \sum_{\beta<\Omega_2} c_\beta$ *are two decompositions of the same element* $b$, *then there exist direct refinements of these decompositions* $b = \sum_{\gamma<\Omega_3} \oplus \bar{a}_\lambda = \sum_{\gamma<\Omega_3} \oplus \bar{c}_\lambda$ *with* $\bar{a}_\lambda \leqq a_\alpha$ *for some* $\alpha = \alpha(\lambda)$ *and* $\bar{c}_\lambda \leqq c_\beta$ *for some* $\beta = \beta(\lambda)$, *and* $\bar{a}_\lambda \sim \bar{c}_\lambda$[7] *for all* $\lambda < \Omega_3$.

PROOF. Replacing $a_\alpha$ by $a'_\alpha = [a_\alpha - (\sum_{\gamma<\alpha} a_\gamma)a_\alpha]$ for $\alpha < \Omega_1$, and $c_\beta$ by $c'_\beta = [c_\beta - (\sum_{\gamma<\beta} c_\gamma)c_\beta]$ for $\beta < \Omega_2$, we have, by Lemma 3.4,

$$b = \sum_{\alpha<\Omega_1} \oplus a'_\alpha = \sum_{\beta<\Omega_2} \oplus c'_\beta,$$

and it is clearly sufficient to prove the lemma for these decompositions. Thus we may (and shall) assume that the given decompositions of $b$ are direct decompositions.

We shall now define a set of decompositions for every $a_\alpha$, $c_\beta$ by transfinite induction. Suppose that for some $\Omega \geqq 1$ the following statements hold for all $0 \leqq \gamma < \Omega$:

$(4)_\gamma$ $a_{\alpha,\lambda}$, $c_{\beta,\lambda}$ *are defined for all* $0 \leqq \lambda \leqq \gamma$, $\alpha < \Omega_1$, $\beta < \Omega_2$,
$a'_{\alpha,\lambda}$, $c'_{\beta,\lambda}$ *are defined for all* $0 \leqq \lambda < \gamma$, $\alpha < \Omega_1$, $\beta < \Omega_2$,

$(5)_\gamma$
$$a_{\alpha,\lambda} = a_{\alpha,\lambda+1} \oplus a'_{\alpha,\lambda} \qquad 0 \leqq \lambda < \gamma, \quad \alpha < \Omega_1,$$
$$c_{\beta,\lambda} = c_{\beta,\lambda+1} \oplus c'_{\beta,\lambda} \qquad 0 \leqq \lambda < \gamma, \quad \beta < \Omega_2,$$

$(6)_\gamma$
$$a_{\alpha,\lambda} = \prod_{\mu<\lambda} a_{\alpha,\mu} \quad \text{if } \lambda \text{ is a limit ordinal} \leqq \gamma, \alpha < \Omega_1,$$
$$c_{\beta,\lambda} = \prod_{\mu<\lambda} c_{\beta,\mu} \quad \text{if } \lambda \text{ is a limit ordinal} \leqq \gamma, \beta < \Omega_2.$$

$(7)_\gamma$
$$a'_{\alpha,\lambda} \neq 0 \quad \text{for exactly one} \quad \alpha = \alpha(\lambda) \quad \text{for} \quad 0 \leqq \lambda < \gamma,$$
$$c'_{\beta,\lambda} \neq 0 \quad \text{for exactly one} \quad \beta = \beta(\lambda) \quad \text{for} \quad 0 \leqq \lambda < \gamma,$$

*and* $a'_{\alpha(\lambda),\lambda} \sim c'_{\beta(\lambda),\lambda}$ *for all* $0 \leqq \lambda < \gamma$,

$(8)_\gamma$ $$b = \sum_{\lambda<\mu} \oplus c'_{\beta(\lambda),\lambda} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\mu} \quad \text{for all } 0 \leqq \mu \leqq \gamma.$$

If $\Omega$ is a limit ordinal, set $a_{\alpha,\Omega} = \prod_{\gamma<\Omega} a_{\alpha,\gamma}$ for $\alpha < \Omega_1$ and $c_{\beta,\Omega} = \prod_{\gamma<\Omega} c_{\beta,\gamma}$ for $\beta < \Omega_2$. It is clear that $(4)_\Omega$, $(5)_\Omega$, $(6)_\Omega$, $(7)_\Omega$ then hold. Furthermore, for every $\gamma < \Omega$,

$$b = \sum_{\lambda<\gamma} \oplus c'_{\beta(\lambda),\lambda} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\gamma} = \sum_{\lambda<\Omega} \oplus c'_{\beta(\lambda),\lambda} + \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\gamma}.$$

---

[7] $a$ is perspective to $c$, in symbols, $a \sim c$, if there exists an element $v$ such that $av = cv = 0$, and $a + v = c + v$. Such a $v$ defines a $(1, 1)$, $<$ – preserving mapping of the elements $a' \leqq a$ on the elements $c' \leqq c$. This mapping is called a perspective mapping and $v$ is called the axis of the perspective mapping.

Hence

$$b = \prod_{\gamma<\Omega}\Big(\sum_{\lambda<\Omega}\oplus c'_{\beta(\lambda),\lambda} + \sum_{\alpha<\Omega_1}\oplus a_{\alpha,\gamma}\Big) = \sum_{\lambda<\Omega}\oplus c'_{\beta(\lambda),\lambda} + \prod_{\gamma<\Omega}\Big(\sum_{\alpha<\Omega_1}\oplus a_{\alpha,\gamma}\Big)$$
$$= \sum_{\lambda<\Omega}\oplus c'_{\beta(\lambda),\lambda} + \sum_{\alpha<\Omega_1}\oplus a_{\alpha,\Omega} \quad \text{by Lemma 3.2.}$$

But

$$\Big(\sum_{\alpha<\Omega_1}\oplus a_{\alpha,\Omega}\Big)\sum_{\lambda<\Omega} c'_{\beta(\lambda),\lambda} = \sum_{\gamma<\Omega}\Big\{\Big(\sum_{\alpha<\Omega_1}\oplus a_{\alpha,\Omega}\Big)\sum_{\lambda<\gamma} c'_{\beta(\lambda),\lambda}\Big\}$$
$$= \sum_{\gamma<\Omega} 0 = 0.$$

Hence $b = \sum_{\lambda<\Omega}\oplus c'_{\beta(\lambda),\lambda}\oplus\sum_{\alpha<\Omega_1}\oplus a_{\alpha,\Omega}$, and $(8)_\Omega$ holds. Thus $(4)_\Omega$–$(8)_\Omega$ hold.

If $\Omega$ is not a limit ordinal let $\gamma$ be its predecessor. If $c_{\beta',\gamma}\neq 0$ for some $\beta'<\Omega_2$, then for this $\beta'$ we have by Lemma 3.1 (using that $c_{\beta',\gamma}\leqq b$) and $(8)_\gamma$, that $c_{\beta',\gamma}S\neq 0$ for some $S=\sum_{r=1}^{N}\oplus a_{\alpha_r,\gamma}\oplus\sum_{r=1}^{M}\oplus c'_{\beta(\lambda_r),\lambda_r}$, with suitable finite $N$, $M$, and $\alpha_r<\Omega_1$ for $r=1,\cdots,N$, and $\lambda_r<\gamma$ for $r=1,\cdots,M$. It is clear that $N>0$ since

$$c_{\beta',\gamma}\sum_{r=1}^{M} c'_{\beta(\lambda_r),\lambda_r} = c_{\beta',\gamma}c_{\beta'}\sum_{r=1}^{M} c'_{\beta(\lambda_r),\lambda_r}$$
$$\leqq c_{\beta',\gamma}\sum_{\lambda<\gamma} c'_{\beta',\lambda} = 0,$$

and we may assume that $N$ is so chosen that $c_{\beta',\gamma}T=0$, where $T=\sum_{r=1}^{N-1}\oplus a_{\alpha_r,\gamma}\oplus\sum_{r=1}^{M}\oplus c'_{\beta(\lambda_r),\lambda_r}$. Now define

$$a_{\alpha,\Omega}=a_{\alpha,\gamma}\qquad a'_{\alpha,\gamma}=0 \qquad \text{if } \alpha\neq\alpha_N,$$
$$a'_{\alpha_N,\gamma}=(c_{\beta',\gamma}+T)a_{\alpha_N,\gamma},\qquad a_{\alpha_N,\Omega}=[a_{\alpha_N,\gamma}-a'_{\alpha_N,\gamma}],$$
$$c'_{\beta,\gamma}=0\qquad c_{\beta,\Omega}=c_{\beta,\gamma} \qquad \text{if } \beta\neq\beta',$$
$$c'_{\beta',\gamma}=c_{\beta',\gamma}S,\qquad c_{\beta',\Omega}=[c_{\beta',\gamma}-c'_{\beta',\gamma}].$$

$(4)_\Omega$, $(5)_\Omega$, $(6)_\Omega$ are clearly satisfied. From its definition, $c'_{\beta',\gamma}$ is not 0; and it is perspective to $a'_{\alpha_N,\gamma}$ with $T$ as axis of perspectivity as shown by the following relations:

$a'_{\alpha_N,\gamma}T\leqq a_{\alpha_N,\gamma}T=0$

$(a_{\alpha_r,\gamma},\ r=1,\cdots,N,\ c'_{\beta(\lambda_r),\lambda_r},\ r=1,\cdots,M$ are independent!),

$c'_{\beta',\gamma}T=0$ (by the choice of $N$),

$$a'_{\alpha_N,\gamma}+T=(c_{\beta',\gamma}+T)a_{\alpha_N,\gamma}+T=(c_{\beta',\gamma}+T)(a_{\alpha_N,\gamma}+T)$$
$$=T+c_{\beta',\gamma}(a_{\alpha_N,\gamma}+T)=T+c_{\beta',\gamma}S=c'_{\beta',\gamma}+T.$$

It then follows that $(7)_\Omega$ holds. Finally,

$$\begin{aligned} b &= \sum_{\lambda<\gamma} \oplus c'_{\beta(\lambda),\lambda} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\gamma} \\ &= \sum_{\lambda<\gamma} \oplus c'_{\beta(\lambda),\lambda} \oplus \sum_{\substack{\alpha<\Omega_1 \\ \alpha\neq\alpha_N}} \oplus a_{\alpha,\Omega} \oplus a_{\alpha_N,\Omega} \oplus a'_{\alpha_N,\gamma} \\ &= \sum_{\lambda<\gamma} \oplus c'_{\beta(\lambda),\lambda} \oplus a'_{\alpha_N,\gamma} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\Omega} \\ &= \sum_{\lambda<\gamma} \oplus c'_{\beta(\lambda),\lambda} \oplus c'_{\beta',\gamma} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\Omega} \\ &= \sum_{\lambda<\Omega} \oplus c'_{\beta(\lambda),\lambda} \oplus \sum_{\alpha<\Omega_1} \oplus a_{\alpha,\Omega}, \end{aligned}$$

and hence $(8)_\Omega$ is satisfied.

Since $(4)_0$–$(8)_0$ are satisfied by $a_{\alpha,0} = a_\alpha$, $\alpha < \Omega_1$, and $c_{\beta,0} = c_\beta$, $\beta < \Omega_2$, it follows that we can continue to define $a_{\alpha,\lambda}$, $a'_{\alpha,\lambda}$, $c_{\beta,\lambda}$, $c'_{\beta,\lambda}$ by transfinite induction to satisfy $(4)_\Omega$–$(8)_\Omega$ until, for some $\Omega$ it happens that all $c_{\beta,\Omega} = 0$. And this must eventually occur since the $c'_{\beta(\lambda),\lambda}$ are distinct elements and hence their cardinal power cannot exceed that of $L$. Thus for some $\Omega$, $(4)_\Omega$–$(8)_\Omega$ hold, but $c_{\beta,\Omega} = 0$ for all $\beta < \Omega_2$. By Lemma 3.3

$$b = \sum_{\beta<\Omega_2} \oplus c_\beta = \sum_{\beta<\Omega_2} \oplus \sum_{\lambda<\Omega} \oplus c'_{\beta,\lambda} = \sum_{\lambda<\Omega} \oplus c'_{\beta(\lambda),\lambda}.$$

$(8)_\Omega$ now implies $a_{\alpha,\Omega} = 0$ for all $\alpha < \Omega_1$, and by Lemma 3.3

$$b = \sum_{\alpha<\Omega_1} \oplus a_\alpha = \sum_{\alpha<\Omega_1} \oplus \sum_{\lambda<\Omega} \oplus a'_{\alpha,\lambda} = \sum_{\lambda<\Omega} \oplus a_{\alpha(\lambda),\lambda}.$$

Since $a_{\alpha(\lambda),\lambda} \leqq a_{\alpha(\lambda)}$, and $c_{\beta(\lambda),\lambda} \leqq c_{\beta(\lambda)}$, for all $\lambda < \Omega$, and $a_{\alpha(\lambda),\lambda} \sim c_{\beta(\lambda),\lambda}$, the theorem is proved.

## 4. Reducible geometries with automorphisms

In this § we shall suppose that $L$ is a (not necessarily irreducible) geometry as described in §2 and that a group $G$ of automorphisms $T$, $S$, $\cdots$ is given such that every element of $G$ maps $L$ into itself in a (1, 1) way preserving the relation $<$ (hence also 0, 1, $+$, $\cdot$, independence of subsystems, and perspectivities). We shall assume that $L$ is irreducible under $G$, that is, if $a$ has a unique complement and $Ta = a$ for all $T$ in $G$, then $a = 0$ or $a = 1$.[8] A congruence relation $\equiv$ depending on $G$ will be defined and its properties studied in this §.

DEFINITION 4.1. *$a \equiv b$ if there exist direct decompositions $a = \sum_{\alpha<\Omega} \oplus a_\alpha$, $b = \sum_{\alpha<\Omega} \oplus b_\alpha$ such that $T_\alpha a_\alpha \sim b_\alpha$ for some $T_\alpha$ in $G$, for all $\alpha < \Omega$.*[9]

[8] The irreducibility of $L$ under $G$ is necessary for Lemma 4.1 and Theorem 4.4, but it is not used in the proofs of Theorems 4.1–4.3. If $G$ consists of only the identity mapping of $L$ on itself, then the condition for irreducibility of $L$ under $G$ becomes the condition for irreducibility of $L$ as formulated by J. v. Neumann (see [1]).

[9] If $G$ consists of only the identity transformation, $a \equiv b$ is a generalisation of the perspectivity by decomposition used in [2], Part I, Chapter IV.

THEOREM 4.1. *The relation* $\equiv$ *is a congruence relation, that is, it is reflexive, symmetric and transitive.*

PROOF. The reflexive ($a \equiv a$ for every $a$) and symmetric ($a \equiv b$ implies $b \equiv a$) properties are immediate from the definition of $\equiv$. To see that $a \equiv b$ and $b \equiv c$ together imply that $a \equiv c$ (transitivity of $\equiv$), let $a = \sum_{\alpha<\Omega_1} \oplus a_\alpha$, $b = \sum_{\alpha<\Omega_1} \oplus b_\alpha = \sum_{\beta<\Omega_2} \oplus b'_\beta$, $c = \sum_{\beta<\Omega_2} \oplus c_\beta$ where $P_\alpha(T_\alpha a_\alpha) = b_\alpha$, $\alpha < \Omega_1$, and $P'_\beta(T'_\beta b'_\beta) = c_\beta$, $\beta < \Omega_2$, for suitable perspectivity mappings $P_\alpha, P'_\beta$. By Theorem 3.1, there exist direct decompositions $b = \sum_{\lambda<\Omega} \oplus \bar{b}_\lambda = \sum_{\lambda<\Omega} \oplus \bar{b}'_\lambda$ such that $\bar{b}_\lambda \sim \bar{b}'_\lambda$ for all $\lambda < \Omega$ and $\bar{b}_\lambda \leqq b_\alpha$ for some $\alpha = \alpha(\lambda)$, $\bar{b}'_\beta \leqq b'_\beta$ for some $\beta = \beta(\lambda)$.

Now let $a'_\lambda = T^{-1}_{\alpha(\lambda)} P^{-1}_{\alpha(\lambda)} \bar{b}_\lambda$ and $c'_\lambda = P'_{\beta(\lambda)} T'_{\beta(\lambda)} \bar{b}'_\lambda$ for $\lambda < \Omega$. Then

$$a = \sum_{\alpha<\Omega_1} \oplus a_\alpha = \sum_{\alpha<\Omega_1} \oplus T^{-1}_\alpha P^{-1}_\alpha b_\alpha = \sum_{\alpha<\Omega_1} \oplus (T^{-1}_\alpha P^{-1}_\alpha \sum_{\alpha(\lambda)=\alpha} \oplus \bar{b}_\lambda)$$

$$= \sum_{\alpha<\Omega_1} \oplus \sum_{\alpha(\lambda)=\alpha} \oplus T^{-1}_\alpha P^{-1}_\alpha \bar{b}_\lambda = \sum_{\alpha<\Omega_1} \oplus \sum_{\alpha(\lambda)=\alpha} \oplus a'_\lambda = \sum_{\lambda<\Omega} \oplus a'_\lambda,$$

that is, $a = \sum_{\lambda<\Omega} \oplus a'_\lambda$. Similarly $c = \sum_{\lambda<\Omega} \oplus c'_\lambda$. Finally $P_{\alpha(\lambda)} T_{\alpha(\lambda)} a'_\lambda = \bar{b}_\lambda$, $\bar{b}_\lambda \sim \bar{b}'_\lambda$, $P'_{\beta(\lambda)} T'_{\beta(\lambda)} \bar{b}'_\lambda = c'_\lambda$, that is, $T'_{\beta(\lambda)} T_{\alpha(\lambda)} a'_\lambda \sim T'_{\beta(\lambda)} \bar{b}_\lambda$, $T'_{\beta(\lambda)} \bar{b}_\lambda \sim T'_{\beta(\lambda)} \bar{b}'_\lambda$, $T'_{\beta(\lambda)} \bar{b}'_\lambda \sim c'_\lambda$. Since perspectivity is transitive, $T''_\lambda a'_\lambda \sim c'_\lambda$, where $T''_\lambda = T'_{\beta(\lambda)} T_{\alpha(\lambda)}$, $\lambda < \Omega$. By Definition 4.1 this implies that $a \equiv c$, as desired.

THEOREM 4.2. *The relation* $\equiv$ *is unrestrictedly additive, that is,* $a_\alpha$, $\alpha < \Omega$, *independent,* $b_\alpha$, $\alpha < \Omega$, *independent, and* $a_\alpha \equiv b_\alpha$ *for all* $\alpha < \Omega$, *together imply* $\sum_{\alpha<\Omega} \oplus a_\alpha \equiv \sum_{\alpha<\Omega} \oplus b_\alpha$.

PROOF. If $a_\alpha = \sum_{\lambda<\Omega(\alpha)} \oplus a_{\alpha,\lambda}$ and $b_\alpha = \sum_{\lambda<\Omega(\alpha)} \oplus b_{\alpha,\lambda}$ with $T_{\alpha,\lambda} a_{\alpha,\lambda} \sim b_{\alpha,\lambda}$ for $\lambda < \Omega(\alpha)$, $\alpha < \Omega$, then

$$\sum_{\alpha<\Omega} \oplus a_\alpha = \sum_{\substack{\lambda<\Omega(\alpha) \\ \alpha<\Omega}} \oplus a_{\alpha,\lambda}, \qquad \sum_{\alpha<\Omega} \oplus b_\alpha = \sum_{\substack{\beta<\Omega(\alpha) \\ \alpha<\Omega}} \oplus b_{\alpha,\lambda},$$

and $T_{\alpha,\lambda} a_{\alpha,\lambda} \sim b_{\alpha,\lambda}$ for $\lambda < \Omega(\alpha)$, $\alpha < \Omega$, which, by Definition 4.1, implies that $\sum_{\alpha<\Omega} \oplus a_\alpha \equiv \sum_{\alpha<\Omega} \oplus b_\alpha$.

DEFINITION 4.2. $a \propto b$ *if* $a \equiv b_1$ *for some* $b_1 < b$.

THEOREM 4.3. *If* $a \equiv b$ *and* $a_1 < a$, *then* $a_1 \propto b$.

PROOF. Let $a = \sum_{\alpha<\Omega} \oplus a_{0,\alpha}$ and $b = \sum_{\alpha<\Omega} \oplus b_{0,\alpha}$ with $P_\alpha T_\alpha a_{0,\alpha} = b_{0,\alpha}$, where the $T_\alpha$ and the $P_\alpha$ are elements of $G$ and perspective mappings respectively. Let $a_2 = [a - a_1] \neq 0$, and apply Theorem 3.1 to the decompositions $a = a_1 \oplus a_2 = \sum_{\alpha<\Omega} \oplus a_{0,\alpha}$ to obtain

$$a = \sum_{\gamma \in I} \oplus a_{1,\gamma} \oplus \sum_{\gamma \in J} \oplus a_{2,\gamma} = \sum_{\gamma \in I} \oplus a'_{0,\gamma} \oplus \sum_{\gamma \in J} \oplus a''_{0,\gamma}$$

with $a_{1,\gamma} \sim a'_{0,\gamma}$, $\gamma \in I$, $a_{2,\gamma} \sim a''_{0,\gamma}$, $\gamma \in J$, $a_{1,\gamma} \leqq a_1$, $\gamma \in I$, $a_{2,\gamma} \leqq a_2$, $\gamma \in J$, $a'_{0,\gamma} \leqq a_{0,\alpha}$ for some $\alpha = \alpha'(\gamma)$, $a''_{0,\gamma} \leqq a_{0,\alpha}$ for some $\alpha = \alpha''(\gamma)$. Set $b_{1,\gamma} = P_{\alpha'(\gamma)} T_{\alpha'(\gamma)} a'_{0,\gamma}$, $b_{2,\gamma} = P_{\alpha''(\gamma)} T_{\alpha''(\gamma)} a''_{0,\gamma}$, and $b_1 = \sum_{\gamma \in I} \oplus b_{1,\gamma}$. Then $b = \sum_{\gamma \in I} \oplus b_{1,\gamma} \oplus \sum_{\gamma \in J} \oplus b_{2,\gamma}$, $a_1 = \sum_{\gamma \in I} \oplus a_{1,\gamma}$, and $b_1 = \sum_{\gamma \in I} \oplus b_{1,\gamma} < b$. Since $a_{1,\gamma} \sim a'_{0,\gamma}$ and $T_{\alpha'(\gamma)} a'_{0,\gamma} \sim b_{1,\gamma}$, it follows from Theorems 4.1 and 4.2 that $a_1 \equiv b_1 < b$ as required.

LEMMA 4.1. *If $a$, $b$ are arbitrary elements but both different from 0, there exist elements $a_1 \leqq a$, $b_1 \leqq b$, different from 0, such that $a_1 \equiv b_1$.*

PROOF.[10] If possible, suppose the lemma false, and let $B = \sum_\alpha b_\alpha$ where $b_\alpha$ runs over all elements $d$ with the property

(*) $\quad a' \equiv d', \quad a' \leqq a, \quad d' \leqq d,$ together imply $a' = d' = 0.$

Then $B$ itself has the property (*). For if $B$ did not have the property (*) there would exist elements $a'$, $d'$, $\neq 0$, such that $Ta' \sim d'$, $a' \leqq a$, $d' \leqq B$, for some $T$ in $G$. By Lemma 3.1, $d'' = d' \sum_{r=1}^{n} b_{\alpha_r} \neq 0$ for some finite $n$. We may suppose that the $\alpha_r$ are chosen so that in addition, $d' \sum_{r=1}^{n-1} b_{\alpha_r} = 0$. Then, since $[b_{\alpha_n} - (\sum_{r=1}^{n-1} b_{\alpha_r}) b_{\alpha_n}] \leqq b_{\alpha_n}$ has the property (*) along with $b_{\alpha_n}$, we may suppose that $b_{\alpha_n} \sum_{r=1}^{n-1} b_{\alpha_r} = 0$. If we now set $b'' = b_{\alpha_n}(d' + \sum_{r=1}^{n-1} b_{\alpha_r})$, we have that $d''$ is perspective to $b''$ with axis of perspectivity $\sum_{r=1}^{n-1} b_{\alpha_r}$, since

$$d'' \sum_{r=1}^{n-1} b_{\alpha_r} = d' \sum_{r=1}^{n-1} b_{\alpha_r} = 0, \qquad b'' \sum_{r=1}^{n-1} b_{\alpha_r} \leqq b_{\alpha_n} \sum_{r=1}^{n-1} b_{\alpha_r} = 0,$$

$$d'' + \sum_{r=1}^{n-1} b_{\alpha_r} = d'\left(b_{\alpha_n} + \sum_{r=1}^{n-1} b_{\alpha_r}\right) + \sum_{r=1}^{n-1} b_{\alpha_r} = \left(d' + \sum_{r=1}^{n-1} b_{\alpha_r}\right)\left(b_{\alpha_n} + \sum_{r=1}^{n-1} b_{\alpha_r}\right)$$

$$= \sum_{r=1}^{n-1} b_{\alpha_r} + b_{\alpha_n}\left(d' + \sum_{r=1}^{n-1} b_{\alpha_r}\right) = b'' + \sum_{r=1}^{n-1} b_{\alpha_r}.$$

Hence, if we set $a'' = T^{-1}d'' \neq 0$, we have $a'' \equiv d''$, $d'' \equiv b''$, implying $a'' \equiv b''$, contradicting (*) for $b_{\alpha_n}$. Hence $B$ has the property (*), and along with it, every $c \leqq B$ has the property (*).

Since $TB$, $T^{-1}B$ have the property (*) along with $B$, $TB \leqq B$ and $T^{-1}B \leqq B$, implying $TB = B$, for all $T$ in $G$. But $B \geqq b \neq 0$ shows that $B \neq 0$, and since $B \geqq a$ is impossible, for $a$ does not have the property (*), $B \neq 1$. From the irreducibility of $L$ under $G$ it follows that $B$ has more than one complement, that is, $B \oplus B_1 = 1$, and $B \oplus B_2 = 1$, for elements $B_1 \neq B_2$. If we set $B_2' = [B_2 - B_1B_2]$ and $B' = (B_1 + B_2)B$ then $B_2'$ is perspective to $B'$ with axis of perspectivity $B_1$, for

$$B_2'B_1 \leqq B_2'B_2B_1 = 0, \qquad B'B_1 \leqq BB_1 = 0,$$

$$B' + B_1 = (B_1 + B_2)B + B_1 = (B_1 + B_2)(B_1 + B) = B_1 + B_2 = B_2' + B_1.$$

Since $B_2'$ thus has the property (*) along with $B'$, it follows that $B_2' \leqq B$, which however contradicts the relations $B_2' \neq 0$, $B_2'B = B_2'B_2B = 0$. Thus the assumption that the lemma is false leads to a contradiction.

THEOREM 4.4. *The relation $\equiv$ is a comparability relation in $L$, that is, for any two elements $a$, $b$ in $L$, at least one of the relations $a \propto b$, $b \propto a$, $a \equiv b$ holds.*

---

[10] The proofs of Lemma 4.1 and Theorem 4.4 follow closely the proofs for the corresponding propositions in [2], Part I.

PROOF. Suppose that for some ordinal $\Omega$ the following statements hold for all $0 \leqq \gamma < \Omega$:

$(9)_\gamma$ $a_\alpha, b_\alpha$ *have been defined for* $0 \leqq \alpha \leqq \gamma$, $a'_\alpha \neq 0, b'_\alpha \neq 0$ *have been defined for* $0 \leqq \alpha < \gamma$ *with* $a'_\alpha \equiv b'_\alpha$ *for* $0 \leqq \alpha < \gamma$.

$(10)_\gamma$ $$a = \sum_{\alpha<\gamma} \oplus a'_\alpha \oplus a_\gamma, \qquad b = \sum_{\alpha<\gamma} \oplus b'_\alpha \oplus b_\gamma.$$

Then if $\Omega$ is a limit ordinal we can define $a_\Omega = \sum_{\gamma<\Omega} a_\gamma$, $b_\Omega = \sum_{\gamma<\Omega} b_\gamma$ and $(9)_\Omega$, $(10)_\Omega$ will be satisfied. If $\Omega$ has a predecessor $\gamma$, and $a_\gamma$, $b_\gamma$ are both different from 0, then by Lemma 4.1 there exist elements $\neq 0$, $a'_\gamma \leqq a_\gamma$ and $b'_\gamma \leqq b_\gamma$ with $a'_\gamma \equiv b'_\gamma$. If we set $a_\Omega = [a_\gamma - a'_\gamma]$ and $b_\Omega = [b_\gamma - b'_\gamma]$ it is clear that $(9)_\Omega$, $(10)_\Omega$ will be satisfied. Since $(9)_0$, $(10)_0$ are trivially satisfied by $a_0 = a$ and $b_0 = b$, it follows that we can continue to define $a_\alpha$, $a'_\alpha$, $b_\alpha$, $b'_\alpha$ by induction, to satisfy $(9)_\gamma$, $(10)_\gamma$ for all $\gamma \leqq \Omega$, until at least one of $a_\Omega$, $b_\Omega$, say $b_\Omega$, $= 0$. And this must eventually occur for some $\Omega$ since the $a'_\alpha$ are all distinct and their cardinal power cannot exceed that of $L$. Then by Theorem 4.2 we have $b = \sum_{\alpha<\Omega} \oplus b'_\alpha \equiv \sum_{\alpha<\Omega} \oplus a'_\alpha \leqq a$, that is, $b \propto a$ or $b \equiv a$. This proves the theorem.

## 5. Dimensionality in reducible geometries

In this § we shall suppose that $L$ is a geometry which is irreducible under a group $G$ as described in §§2, 3, 4. We shall further postulate that $L$ is finite under $G$, that is, $1 \equiv a$ (see Definition 4.1) holds only if $a = 1$.[11]

LEMMA 5.1. *If* $a \equiv b$ *and* $a \leqq b$ *then* $a = b$.

PROOF. If we set $c = [1 - b]$, Theorem 4.2 shows that $1 = b \oplus c \equiv a \oplus c$. Hence $a + c = 1$ and $b = b(a + c) = a + bc = a$.

THEOREM 5.1. *For any two elements* $a$, $b$ *in* $L$ *exactly one of the relations* $a \propto b$, $b \propto a$, $a \equiv b$ *holds.*

PROOF. By Theorem 4.4 at least one of these relations holds. If more than one of them held, then Definition 4.2, Theorem 4.3 and Theorem 4.1 would imply that $a \equiv a_1$ for some $a_1 < a$, which is impossible by Lemma 5.1.

LEMMA 5.2. *If* $b \neq 0$ *and* $a_r$, $1 \leqq r < p$, *are independent, then* $a_r \equiv b$ *for* $1 \leqq r < p$ *implies that* $p$ *is finite.*

PROOF. If $p$ were infinite, Theorem 4.1 would give $a_r \equiv a_{r+1}$ for $r \geqq 1$, and Theorem 4.2 would imply that

$$\sum_{r=1}^{\infty} \oplus a_r \equiv \sum_{r=2}^{\infty} \oplus a_r < \sum_{r=1}^{\infty} \oplus a_r,$$

which is impossible by Lemma 5.1. Thus $p$ must be finite.

[11] Although the definition of the relation $\equiv$ involves both the group $G$ of the transformations of $L$ and the perspectivities in $L$, the finiteness condition (which can be violated in some geometries, as shown by examples similar to the ones constructed in §6) is a condition on the transformations rather than on the perspectivities. This is due to the fact that perspectivity is unrestrictedly additive in reducible as well as irreducible geometries, as will be shown elsewhere.

We can now follow almost literally the method of von Neumann for defining a numerical dimension function. By means of Theorem 5.1, Lemma 5.2 and Lemma 5.1 we prove the following lemma.

LEMMA 5.3. *If $a$, $b$ are elements of $L$ with $b \neq 0$, there exists a decomposition $a = \sum_{r=1}^{n} \oplus a_r' + a_n$ with $a_r' \equiv b$ for $1 \leqq r \leqq n$, $n = 0, 1, 2, \cdots$, and $a_n \propto b$. The finite integer $n = [a:b]$ depends only on the elements $a$, $b$ and not on the particular decomposition of $a$.*

Suppose now that there is an element $b \neq 0$ in $L$ such that $0 \leqq b_1 < b$ implies $b_1 = 0$ (such a $b$ is called a minimal element). (Then $a_n = 0$ in Lemma 5.4.) If, using this $b$ we set $D(a) = [a:b]$ we obtain a numerical function defined for all $a$ in $L$ with $0 \leqq D(a) \leqq 1$, and $D(a) = 0(1)$ if and only if $a = 0(1)$. From Theorems 5.1 and 4.2 it follows that $D(a) <, >, = D(c)$ according as $a \propto c$, $c \propto a$, or $a \equiv c$. From Theorem 4.2 it also follows that $D(\sum_\alpha \oplus a_\alpha) = \sum_\alpha D(a_\alpha)$, $D(\sum_\alpha a_\alpha) = \lim_\alpha D(\sum_{\beta<\alpha} a_\beta)$, $D(\prod_\alpha a_\alpha) = \lim_\alpha D(\prod_{\beta<\alpha} a_\beta)$, hence for all $a$, $c$ $D(a + c) + D(ac) = D(a) + D([c - ac]) + D(ac) = D(a) + D(c)$. It is easily seen that in this case (existence of a minimal element) the range of $D(a)$ is the set of real numbers $0, 1/N, 2/N, \cdots, N/N$ for some $N = 1, 2, 3, \cdots$, and that $L$ is a direct sum of a finite number of isomorphic projective geometries under a group $G$ which permutes the geometries.

If there is no minimal element in $L$ then every $b \neq 0$ can be expressed as $b = b_1 \oplus b_2$ with $b_1 \neq 0$, $b_2 \neq 0$. It follows that if $b \neq 0$ there is a $b'$ (one of $b_1$ or $b_2$ will do) such that $[b:b'] \geqq 2$. Similarly, there is a sequence $b_1, b_2, \cdots$ with $[b_n:b_{n+1}] \geqq 2$ (such a sequence is called a minimal sequence). It can be shown that $\lim_{n\to\infty} [a:b_n]/[1:b_n]$ exists for every $a$ in $L$. If we set $D(a) =$ this limit it can be shown that $D(a)$ is a numerical function, $0 \leqq D(a) \leqq 1$, defined for all $a$ in $L$, that $D(a) = 0(1)$ if and only if $a = 0(1)$, that $D(a) <, >, = D(c)$ according as $a \propto c$, $c \propto a$, or $a \equiv c$, and that $D(\sum_\alpha \oplus a_\alpha) = \sum_\alpha D(a_\alpha)$, $D(\sum_\alpha a_\alpha) = \lim_\alpha D(\sum_{\beta<\alpha} a_\beta)$, $D(\prod_\alpha a_\alpha) = \lim_\alpha D(\prod_{\beta<\alpha} a_\beta)$, $D(a + c) + D(ac) = D(a) + D(c)$ for all $a$, $c$ in $L$. From the completeness of $L$ it follows that in this case (existence of a minimal sequence) the range of $D(a)$ is the set of all real numbers in the interval $0 \leqq x \leqq 1$. This case clearly arises for the direct sum of a finite number of isomorphic continuous geometries under a suitable group of permutations of the geometries. A less trivial realization of this case is the integrated sum of isomorphic (projective or continuous) irreducible geometries as described in the next §.

In both of the above cases it is clear from the construction of $D(a)$ that it is the unique unrestrictedly additive dimension function which is invariant under $G$, normalized by the condition $D(1) = 1$.

## 6. Integrated sums of geometries

In this § $L$ will denote an arbitrary geometry which is finite and irreducible under a group $G$, as described in §§2, 3, 4, 5, $D(a)$ will be the normalized ($D(0) = 0, D(1) = 1$) dimension function as defined in §5, and $S$ will denote an arbitrary space of points $x$ with a Lebesgue measure function $\mu$ such that

$\mu(S) > 0, < \infty$. By means of the metric $d(a, b)$ introduced by von Neumann, we shall define measurable functions $f(x)$ with values in $L$ for $x$ in $S$, of which the equivalence classes will again form a geometry—the integrated sum of $L$ over $S$—which is finite and irreducible under a suitable group. If $L$ is chosen to be an arbitrary irreducible (projective or continuous) geometry, this enables us to construct an extensive class of reducible geometries.

LEMMA 6.1.[12] *The numerical function* $d(a, b) = D(a + b) - D(ab)$ *is a distance function in* $L$, *i.e.,* $d(a, b) = d(b, a) > 0$ *if* $a \neq b$, $d(a, a) = 0$, $d(a, b) \leqq d(a, c) + d(c, b)$, *for all* $a, b, c$ *in* $L$. *Furthermore* $d(a + c, b + c) \leqq d(a, b)$ *and* $d(ac, bc) \leqq d(a, b)$ *for all* $a, b, c$ *in* $L$.

PROOF.

$$\begin{aligned} d(a, c) + d(c, b) &= D(a + c) + D(c + b) - D(ac) - D(cb) \\ &= D(a) + D(b) - D(ab) + 2\{D(c) + D(ab) - D(ac) - D(cb)\} \\ &= d(a, b) + 2\{D(c + ab) - D(ac + cb)\} \\ &\geqq d(a, b) \end{aligned}$$

since $ac + cb \leqq c + ab$.

Let $c_1 = c(a + b) \leqq a + b$ and $c_2 = [c - c_1]$. Then $c_2(a + b) = 0$, and

$$\begin{aligned} d(a + c, b + c) &= D(c + a + b) - D((a + c)(b + c)) \\ &= D(c_2 + a + b) - D(c_2 + (a + c_1)(b + c_1)) \\ &= D(c_2) + D(a + b) - D(c_2) - D((a + c_1)(b + c_1)) \\ &\leqq D(a + b) - D(ab) = d(a, b) \end{aligned}$$

since $(a + c_1)(b + c_1) \geqq ab$.

Let $c_1 = cab \leqq ab$ and $c_2 = [c - c_1]$. Then $c_2ab = 0$, and

$$\begin{aligned} d(ac, bc) &= D(ac + bc) - D(cab) = D(c_1 + c_2a + c_2b) - D(c_1) \\ &= D(c_1) + D(c_2a + c_2b) - D(c_1) \leqq D(c_2(a + b)) + D(ab) - D(ab) \\ &\leqq D(a + b) - D(ab) = d(a, b) \end{aligned}$$

since $c_2(a + b) \oplus ab \leqq a + b$.

The other parts of the lemma follow immediately from the definition of $d(a, b)$.

LEMMA 6.2.

$$d\left(a, \prod_{n=1}^{\infty} b_n\right) = \lim_{p \to \infty} d\left(a, \prod_{n=1}^{p} b_n\right) \leqq d(a, b_1) + \sum_{n=1}^{\infty} d(b_n, b_{n+1}),$$

*and*

$$d\left(a, \sum_{n=1}^{\infty} b_n\right) = \lim_{p \to \infty} d\left(a, \sum_{n=1}^{p} b_n\right) \leqq d(a, b_1) + \sum_{n=1}^{\infty} d(b_n, b_{n+1}).$$

[12] Lemmas 6.1–6.3 were given by von Neumann (see [1]).

PROOF. Using Lemma 6.1 we derive

$$\begin{aligned} d\left(a, \prod_{n=1}^{\infty} b_n\right) &= D\left(a + \prod_{n=1}^{\infty} b_n\right) - D\left(a \prod_{n=1}^{\infty} b_n\right) \\ &= \lim_{p\to\infty}\left\{D\left(a + \prod_{n=1}^{p} b_n\right) - D\left(a \prod_{n=1}^{p} b_n\right)\right\} \\ &= \lim_{p\to\infty} d\left(a, \prod_{n=1}^{p} b_n\right) \\ &\leqq \lim_{p\to\infty} \{d(a, b_1) + d(b_1, b_1b_2) + \cdots + d(b_1 \cdots b_p, b_1 \cdots b_pb_{p+1})\} \\ &\leqq \lim_{p\to\infty} \{d(a, b_1) + d(b_1, b_2) + \cdots + d(b_p, b_{p+1})\} \\ &= d(a, b_1) + \sum_{p=1}^{\infty} d(b_p, b_{p+1}), \end{aligned}$$

proving the first part of the lemma. The second part can be proved in a similar way.

LEMMA 6.3. *$L$ is a complete metric space under the distance function $d(a, b)$, that is, if $a_1, a_2, \cdots$ satisfy $d(a_n, a_m) \to 0$ as $n, m \to \infty$, then there exists an element $a$ such that $d(a, a_n) \to 0$ as $n \to \infty$. Furthermore, if $\sum_{n=1}^{\infty} d(a_n, a_{n+1}) < \infty$, then $a = \sum_{p=1}^{\infty} \prod_{n=p}^{\infty} a_n = \prod_{p=1}^{\infty} \sum_{n=p}^{\infty} a_n$.*

PROOF. Let $d(a_n, a_m) \to 0$ as $n, m \to \infty$, and let $n_r, r = 1, 2, \cdots$ be chosen so that $n_r < n_{r+1}$ and $\sum_{r=1}^{\infty} d(a_{n_r}, a_{n_{r+1}}) < \infty$, which can clearly be done. Let $a = \sum_{p=1}^{\infty} \prod_{r=p}^{\infty} a_{n_r}$, and $\bar{a} = \prod_{p=1}^{\infty} \sum_{r=p}^{\infty} a_{n_r}$. Then, using Lemma 6.2, we derive

$$\begin{aligned} \lim_{r\to\infty} d(a_r, a) &\leqq \lim_{r\to\infty} d(a_r, a_{n_r}) + \lim_{r\to\infty} d(a_{n_r}, a) \\ &= 0 + \lim_{r\to\infty} \lim_{p\to\infty} d\left(a_{n_r}, \prod_{i=p}^{\infty} a_{n_i}\right) \\ &\leqq \overline{\lim_{p\to\infty}} \sum_{r=p}^{\infty} d(a_{n_r}, a_{n_{r+1}}) = 0. \end{aligned}$$

By similar reasoning, $\lim_{r\to\infty} d(a_r, \bar{a}) = 0$ can be established. Hence

$$\begin{aligned} d(a, \bar{a}) &\leqq \overline{\lim_{r\to\infty}} \{d(a, a_r) + d(a_r, \bar{a})\} \\ &\leqq \overline{\lim_{r\to\infty}} d(a, a_r) + \overline{\lim_{r\to\infty}} d(a_r, \bar{a}) \\ &= 0 + 0 = 0 \quad \text{and} \quad a = \bar{a}. \end{aligned}$$

DEFINITION 6.1. *A function $f(x)$ with values in $L$ and defined for almost all $x$ in $S$ is measurable if for every $\eta > 0$,*

(11) *$E_x[d(f(x), a) < \eta]$ is measurable for every $a$ in $L$, and*

(12) *there exists a finite or countable sequence* $a_1, a_2, \cdots$ *such that* $\mu\{S - \sum_n E_x[d(f(x), a_n) < \eta]\} = 0$.[13]

DEFINITION 6.2. *A function* $f(x)$ *is countably valued if there exists a finite or countable sequence* $a_1, a_2, \cdots$ *such that*

(13) $E_x[f(x) = a_n]$ *is measurable for* $n = 1, 2, \cdots$, *and*

(14) $\mu\{S - \sum_n E_x[f(x) = a_n]\} = 0$.[13]

LEMMA 6.4. *Every countably valued* $f(x)$ *is measurable.*

PROOF. If $f(x)$ is countably valued as defined in Definition 6.2 and $\eta > 0$, $a$ in $L$ are given, then $E_x[d(f(x), a) < \eta] = \sum_{d(a_n,a)<\eta} E_x[f(x) = a_n]$ = an at most countable sum of measurable sets = measurable set. This verifies (11). (12) follows immediately from (14).

LEMMA 6.5. *If for almost all* $x$, $f_1(x) \leqq f_2(x) \leqq \cdots$ $(f_1(x) \geqq f_2(x) \geqq \cdots)$, *where the functions are all measurable, then the function* $f(x)$ *defined for almost all* $x$ *by* $f(x) = \sum_{n=1}^{\infty} f_n(x)$ $(\prod_{n=1}^{\infty} f_n(x))$ *is measurable.*

PROOF. If $\eta > 0$, and $a$ in $L$ are given, then

$$E_x[d(f(x), a) < \eta] = \sum_{\substack{m=1 \\ m>\frac{1}{\eta}}}^{\infty} \sum_{p=1}^{\infty} \prod_{n=p}^{\infty} E_x\left[d(f_n(x), a) < \left(\eta - \frac{1}{m}\right)\right]$$

= a measurable set. Furthermore, if

$$\mu\left\{S - \sum_{m=1}^{\infty} E_x[d(f_n(x), a_{n,m}) < \tfrac{1}{2}\eta]\right\} = 0, \qquad n = 1, 2, \cdots,$$

then $\mu(S - T) = 0$ where $T = \prod_{n=1}^{\infty} \sum_{m=1}^{\infty} E_x[d(f_n(x), a_{n,m}) < \frac{1}{2}\eta]$. Since for almost all $x$ in $T$, $d(f(x), f_n(x)) < \frac{1}{2}\eta$ for $n = n(x)$ sufficiently large, it follows that for almost all $x$ in $T$, for suitable $n$, $m$,

$$d(f(x), a_{n,m}) \leqq d(f(x), f_n(x)) + d(f_n(x), a_{n,m}) < \tfrac{1}{2}\eta + \tfrac{1}{2}\eta = \eta.$$

Hence $\mu\{S - \sum_{n,m=1}^{\infty} E_x[d(f(x), a_{n,m}) < \eta]\} = 0$, and $f(x)$ is measurable.

THEOREM 6.1. $f(x)$ *is measurable if and only if there exists a set of countably valued functions* $f_n(x)$ *such that for almost all* $x$, $f(x) = \prod_{p=1}^{\infty} \sum_{n=p}^{\infty} f_n(x)$ $(f(x) = \sum_{p=1}^{\infty} \prod_{n=p}^{\infty} f_n(x))$.

PROOF. If such countably valued, hence measurable, functions do exist, then $f(x)$ is measurable by a repeated application of Lemma 6.5. Conversely, if $f(x)$ is measurable, let $a_{n,m}$ be such that $\mu\{S - \sum_{m=1}^{\infty} E_x[d(f(x), a_{n,m}) < 1/n^2]\} = 0$ for $n = 1, 2, \cdots$. Define $f_n(x)$ for almost all $x$ by $f_n(x) = a_{n,m(n,x)}$ where $m(n, x)$ is the first $m$ for which $d(f(x), a_{n,m}) < 1/n^2$. It is clear that $f_n(x)$ is countably valued and that $d(f(x), f_n(x)) < 1/n^2$ for almost all $x$. The theorem now follows from Lemma 6.3, since

$$\sum_{n=1}^{\infty} d(f_n(x), f_{n+1}(x)) \leqq \sum_{n=1}^{\infty} d(f(x), f_n(x)) + \sum_{n=1}^{\infty} d(f(x), f_{n+1}(x)) < \infty.$$

---

[13] $E_x[P(x)]$ denotes the set of points $x$ with the property $P(x)$.

LEMMA 6.6. *If $f(x)$, $g(x)$ are countably valued, then $f(x) + g(x)$ and $f(x)g(x)$ are countably valued.*

PROOF. If $a_1, a_2, \cdots$ and $b_1, b_2, \cdots$ are the sequences which satisfy (13), (14) for $f(x)$, $g(x)$ respectively, then $a_n + b_m$, $n, m = 1, 2, \cdots$, and $a_n b_m$, $n, m = 1, 2, \cdots$ satisfy (13), (14) for $f(x) + g(x)$ and $f(x)g(x)$ respectively. For, neglecting $\mu$-null sets,

$$E_x[f(x) + g(x) = a_n + b_m] = \sum_{a_r + b_s = a_n + b_m} E_x[f(x) = a_r] E_x[g(x) = b_s]$$

= measurable set for $n, m = 1, 2, \cdots$, and

$$\mu\left\{S - \sum_{n,m=1}^{\infty} E_x[f(x) + g(x) = a_n + b_m]\right\}$$

$$= \mu\left\{S - \sum_{n=1}^{\infty} E_x[f(x) = a_n] \sum_{m=1}^{\infty} E_x[g(x) = b_m]\right\}$$

$$= 0,$$

proving the part of the lemma concerning $f(x) + g(x)$. The rest of the lemma can be shown in a similar way.

THEOREM 6.2. *If $f(x)$, $g(x)$ are measurable, then $f(x) + g(x)$, $f(x)g(x)$ are measurable.*

PROOF. If $f_n(x)$, $g_n(x)$ are countably valued functions as described in Theorem 6.1 for $f(x)$, $g(x)$ respectively, then $f_n(x) + g_m(x)$, $n, m = 1, 2, \cdots$, and $f_n(x)g_m(x)$, $n, m = 1, 2, \cdots$, are countably valued functions (by Lemma 6.6) for $f(x) + g(x)$ and $f(x)g(x)$ respectively. For, using the continuity axiom,

$$f(x) + g(x) = \prod_{p=1}^{\infty} \sum_{n=p}^{\infty} f_n(x) + \prod_{q=1}^{\infty} \sum_{m=q}^{\infty} g_m(x)$$

$$= \prod_{p,q=1}^{\infty} \left\{\sum_{n=p}^{\infty} f_n(x) + \sum_{m=q}^{\infty} g_m(x)\right\}$$

$$= \prod_{p,q=1}^{\infty} \sum_{n=p}^{\infty} \sum_{m=q}^{\infty} \{f_n(x) + g_m(x)\},$$

$$f(x)g(x) = \sum_{p=1}^{\infty} \prod_{n=p}^{\infty} f_n(x) \sum_{q=1}^{\infty} \prod_{m=q}^{\infty} g_m(x)$$

$$= \sum_{p,q=1}^{\infty} \prod_{n=p}^{\infty} \prod_{m=q}^{\infty} \{f_n(x) g_m(x)\}.$$

COROLLARY. *If $f(x)$, $g(x)$ are measurable, then $D(f(x))$, $D(f(x) + g(x))$, $D(f(x)g(x))$, and $d(f(x), g(x))$ are numerical measurable functions, and $E_x[f(x) < g(x)]$, $E_x[f(x) = g(x)]$ are measurable sets.*

PROOF. It is clear that $D(f(x))$ is measurable if $f(x)$ is countably valued. If now $f(x)$ is merely measurable, and $f_n(x)$ are the countably valued functions existing by Theorem 6.1, then $D(f(x)) = D\left(\prod_{p=1}^{\infty} \sum_{n=p}^{\infty} f_n(x)\right) = \lim_{p\to\infty} \lim_{q\to\infty}$

$D\left(\sum_{n=p}^{q} f_n(x)\right)$ = measurable function. Since $f(x)$, $g(x)$ measurable imply $f(x) + g(x)$, $f(x)g(x)$ measurable, it follows that $D(f(x) + g(x))$ and $D(f(x)g(x))$ are measurable. Finally, $d(f(x), g(x)) = D(f(x) + g(x)) - D(f(x)g(x))$ is measurable, and $E_x[f(x) = g(x)] = E_x[D(f(x)) = D(g(x)) = D(f(x) + g(x))]$, and $E_x[f(x) < g(x)] = E_x[D(f(x) + g(x)) = D(g(x)), f(x) \neq g(x)]$ are measurable.

DEFINITION 6.3. *If $f(x)$ is measurable, the equivalence class of all functions $f_1(x)$ such that $f_1(x) = f(x)$ almost everywhere is denoted by $J = J(f)$. The set of all such $J$ is denoted by $\mathfrak{L}$.*

LEMMA 6.7. *The set of all measurable $f(x)$ consists of mutually exclusive equivalence classes. $J(f(x) + g(x))$, $J(f(x)g(x))$, which are defined by Theorem 6.2 if $f(x)$, $g(x)$ are measurable, depend only on the equivalence classes of $f(x)$, $g(x)$, and not on the particular $f(x)$, $g(x)$.*

PROOF. This follows immediately from the properties of null sets and Definition 6.3.

DEFINITION 6.4. *A relation $<$ is defined in $\mathfrak{L}$ as follows: $J_1 < J_2$ if and only if $J_1 = J(f_1(x))$, $J_2 = J(f_2(x))$, where $f_1(x) \leqq f_2(x)$ for almost all $x$, and $f_1(x) < f_2(x)$ on a set of positive measure.*

LEMMA 6.8. *$J_1 \leqq J_2$, that is, $J_1 < J_2$ or $J_1 = J_2$, if and only if $J_1 = J(f_1(x))$, $J_2 = J(f_2(x))$, where $f_1(x) \leqq f_2(x)$ almost everywhere.*

PROOF. This follows immediately from Definitions 6.3 and 6.4 and the fact that $E_x[f_1(x) < f_2(x)]$ is measurable, by the corollary to Theorem 6.2, if $f_1(x)$, $f_2(x)$ are measurable.

THEOREM 6.3. *$\mathfrak{L}$ is partially ordered under the relation $<$.*

PROOF. From Definition 6.4 it is clear that $J < J$ never holds. If $J(f_1(x)) < J(f_2(x))$ and $J(f_2(x)) < J(f_3(x))$, then $f_1(x) \leqq f_2(x)$, $f_2(x) \leqq f_3(x)$, implying $f_1(x) \leqq f_3(x)$, almost everywhere, and $f_1(x) < f_2(x)$, hence $f_1(x) < f_3(x)$, on a set of positive measure, implying that $J(f_1(x)) < J(f_3(x))$. This means that $\mathfrak{L}$ is partially ordered.

THEOREM 6.4. *$\mathfrak{L}$ is complete with respect to the relation $<$, that is, if $J_\alpha$, $\alpha \in I$, is an arbitrary set of elements in $\mathfrak{L}$, there exist elements in $\mathfrak{L}$, $J^{(1)} = \sum_{\alpha \in I} J_\alpha$, $J^{(2)} = \prod_{\alpha \in I} J_\alpha$, such that for any $J$ in $\mathfrak{L}$, $J^{(1)} \leqq J$ is equivalent to $J_\alpha \leqq J$ for all $\alpha \in I$, and $J \leqq J^{(2)}$ is equivalent to $J \leqq J_\alpha$ for all $\alpha \in I$. Furthermore, there exist finite or countable subsets $I_1$, $I_2$ of $I$, such that $\sum_{\alpha \in I} J_\alpha = \sum_{\alpha \in I_1} J_\alpha$, $\prod_{\alpha \in I} J_\alpha = \prod_{\alpha \in I_2} J_\alpha$.*

PROOF. Let $J_\alpha = J(f_\alpha(x))$. If $I$ is finite or countably infinite, it follows from Theorem 6.2 and Lemma 6.5 that $f^{(1)}(x) = \sum_\alpha f_\alpha(x) = \sum_{n=1}^{\infty} \sum_{r=1}^{n} f_r(x)$ is measurable, and from the familiar property of null sets of being countably additive, it follows that $J(f^{(1)}(x)) = \sum_{\alpha \in I} J(f_\alpha(x))$. If now $I$ is not countable, let $D = \overline{\text{bd}}. \int_S D\left(\sum_{i=1}^{N} f_{\alpha_i}(x)\right) d\mu(x)$, where all finite sums of the $f_\alpha(x)$ are considered. Clearly $0 \leqq D \leqq \mu(S)$. Choose $f_{\alpha_{n,r}}(x) \in I$ so that $\int_S D\left(\sum_{r=1}^{N(n)} f_{\alpha_{n,r}}(x)\right) d\mu(x) > D - 1/n$, for $n = 1, 2, \cdots$, which can clearly be done. Let $f^{(1)}(x) = \sum_{n=1}^{\infty} \sum_{r=1}^{N(n)} f_{\alpha_{n,r}}(x)$, and $J^{(1)} = J(f^{(1)}(x))$. Then

clearly $\int_S D(f_\alpha(x) + f^{(1)}(x))\,d\mu(x) = \int_S D(f^{(1)}(x))\,d\mu(x) = D$, which means $f_\alpha(x) \leqq f^{(1)}(x)$ for almost all $x$, that is, $J_\alpha \leqq J^{(1)}$, for all $\alpha \in I$. Hence, for any $J$ in $\mathfrak{L}$, $J^{(1)} \leqq J$ implies $J_\alpha \leqq J$ for all $\alpha \in I$. Conversely, if $J_\alpha \leqq J = J(f(x))$ for all $\alpha \in I$, then in particular $J_{\alpha_{n,r}} \leqq J$ for all $n$, $r$. Hence, except for a countable sum of null sets, which is again a null set, we have for all $x$, for all $n, r$, $f_{\alpha_{n,r}}(x) \leqq f(x)$, and therefore $f^{(1)}(x) = \sum_{n=1}^{\infty} \sum_{r=1}^{N(n)} f_{\alpha_{n,r}}(x) \leqq f(x)$, implying $J^{(1)} \leqq J$. Thus $J^{(1)}$ satisfies the requirements of the theorem.

In a similar way, by considering $\underline{\mathrm{bd}} \int_S D\left(\prod_{i=1}^{N} f_{\alpha_i}(x)\right) d\mu(x)$, $J^{(2)}$ can be defined and can be shown to satisfy the requirements of the theorem.

THEOREM 6.5. *$\mathfrak{L}$ is continuous with respect to the relation $<$, that is, if $J$, $J_\alpha$, $\alpha < \Omega$, are elements in $\mathfrak{L}$, where $\Omega$ is an arbitrary ordinal, then $J \sum_{\alpha<\Omega} J_\alpha = \sum_{\gamma<\Omega} (J \sum_{\alpha<\gamma} J_\alpha)$, and $J + \prod_{\alpha<\Omega} J_\alpha = \prod_{\gamma<\Omega} (J + \prod_{\alpha<\gamma} J_\alpha)$.*

PROOF. If the cardinal power of the set of $\alpha < \Omega$ is not countable, it follows from Theorem 6.4 that $\sum_{\alpha<\Omega} J_\alpha = \sum_{\alpha<\gamma_1} J_\alpha$, $\prod_{\alpha<\Omega} J_\alpha = \prod_{\alpha<\gamma_2} J_\alpha$, for suitable ordinals $\gamma_1, \gamma_2 < \Omega$, and the theorem follows. If $\Omega$ is countable, let $J = J(f(x))$, $J_\alpha = J(f_\alpha(x))$. Then, as in the proof of Theorem 6.4,

$$\begin{aligned} J \sum_{n=1}^{\infty} J_n &= J(f(x)) \sum_{n=1}^{\infty} J(f_n(x)) = J(f(x) \sum_{n=1}^{\infty} f_n(x)) \\ &= J\left(\sum_{p=1}^{\infty} (f(x) \sum_{n=1}^{p} f_n(x))\right) = \sum_{p=1}^{\infty} J(f(x) \sum_{n=1}^{p} f_n(x)) \\ &= \sum_{p=1}^{\infty} (J(f(x)) \sum_{n=1}^{p} J(f_n(x))) = \sum_{p=1}^{\infty} (J \sum_{n=1}^{p} J_n), \end{aligned}$$

as required. Similarly, $J + \prod_{n=1}^{\infty} J_n = \prod_{p=1}^{\infty} (J + \prod_{n=1}^{p} J_n)$.

THEOREM 6.6. *$\mathfrak{L}$ is modular with respect to the relation $<$, that is, $J_1 \leqq J_2$ implies $J_2(J_1 + J_3) = J_1 + J_2 J_3$.*

PROOF. Let $J_1 = J(f_1(x))$, $J_2 = J(f_2(x))$, and $J_3 = J(f_3(x))$. Then $J_1 \leqq J_2$ implies that $f_1(x) \leqq f_2(x)$ for almost all $x$, and hence $J_2(J_1 + J_3) = (J(f_2(x)))(J(f_1(x)) + J(f_3(x))) = J(f_2(x)(f_1(x) + f_3(x))) = J(f_1(x) + f_2(x)f_3(x))$ $= J(f_1(x)) + J(f_2(x))J(f_3(x)) = J_1 + J_2 J_3$, as required.

LEMMA 6.9. *If $a_1$, $a_2$, $a_3$ are elements in $L$ for which $a_1 \oplus a_2 = 1$ and $d(a_1, a_3) < \eta$, then there exists an element $a_4$ in $L$ for which $a_3 \oplus a_4 = 1$ and $d(a_2, a_4) < \eta$.*

PROOF. Let $a_4 = [a_2 - (a_1 + a_3)a_2] \oplus [a_1 - a_1 a_3]$. Then

$$\begin{aligned} a_3 + a_4 &= a_3 + [a_1 - a_1 a_3] + [a_2 - (a_1 + a_3)a_2] = \\ &= a_3 + a_1 + [a_2 - (a_1 + a_3)a_2] = a_3 + a_1 + a_2 = 1, \end{aligned}$$

$$a_3 a_4 = a_3(a_1 + a_3)a_4 = a_3[a_1 - a_1 a_3]a_4 = 0, \text{ and}$$

$$\begin{aligned} d(a_2, a_4) &= D(a_2 + [a_1 - a_1 a_3]) - D([a_2 - (a_1 + a_3)a_2]) \\ &= D(a_2) + D(a_1) - D(a_1 a_3) - D(a_2) + D((a_1 + a_3)a_2) \\ &= D(a_1) - D(a_1 a_3) + D(a_1 + a_3) + D(a_2) - D(a_1 + a_3 + a_2) \\ &= D(a_1 + a_3) - D(a_1 a_3) = d(a_1, a_3) < \eta, \end{aligned}$$

proving the lemma.

THEOREM 6.7. *$\mathfrak{L}$ is complemented, that is, if $J$ is an arbitrary element in $\mathfrak{L}$, then there exists an element $J'$ in $\mathfrak{L}$ such that $J \oplus J' = 1$ in $\mathfrak{L}$.*

PROOF. Let $J = J(f(x))$ where $f(x) = \prod_{p=1}^{\infty} \sum_{n=p}^{\infty} f_n(x)$ with $f_n(x)$ countably valued and $\mu\{S - E_x[d(f(x), f_n(x)) < 1/n^2]\} = 0$, hence $\mu\{S - E_x[d(f_n(x), f_{n+1}(x)) < 2/n^2]\} = 0$, as in the proof of Theorem 6.1. Let $a_{n,m}$, $m = 1, 2, \cdots$, be the sequence of elements in $L$, according to Definition 6.2, for which $\mu\{S - \sum_{m=1}^{\infty} e_{n,m}\} = 0$, where $e_{n,m} = E_x[f_n(x) = a_{n,m}]$. By replacing the $e_{n,m}$, $n, m = 1, 2, \cdots$, by $e_{n,m} \prod_{r=1}^{n-1} e_{r,s_r}$, $n, m = 1, 2, \cdots$, where $s_r$ is allowed to take all values $= 1, 2, \cdots$, we may assume that $e_{n,m} \leqq e_{n-1,r}$ for some $r = r(n, m)$, for all $n = 2, 3, \cdots$. Now let $a'_{n,m}$ be chosen by induction so that $a_{n,m} \oplus a'_{n,m} = 1$ in $L$, and $d(a'_{n,m}, a'_{n-1,r}) \leqq 2/(n-1)^2$, for $n = 2, 3, \cdots$, which can be done by Lemma 6.9. Set $f'_n(x) = a'_{n,m}$ for $x \in e_{n,m}$. Then clearly $d(f'_n(x), f'_{n+1}(x)) \leqq 2/n^2$ for almost all $x$, and we can define $f'(x) = \prod_{p=1}^{\infty} \sum_{n=p}^{\infty} f'_n(x)$, which is measurable by Lemma 6.5, and for which $d(f'_n(x), f'(x)) \to 0$ as $n \to \infty$, for almost all $x$, by Lemma 6.3. Then, for almost all $x$, $d(f(x), f'(x)) \geqq \varliminf_{n\to\infty} \{d(f_n(x), f'_n(x)) - d(f(x), f_n(x)) - d(f'_n(x), f'(x))\} = 1 - 0 - 0 = 1$, implying that $f(x) \oplus f'(x) = 1$ in $L$ for almost all $x$. It follows that for $J' = J(f'(x))$ we have $J + J' = J(f(x)) + J(f'(x)) = J(f(x) + f'(x)) = 1$ in $\mathfrak{L}$, $JJ' = J(f(x))J(f'(x)) = J(f(x)f'(x)) = 0$ in $\mathfrak{L}$, hence $J \oplus J' = 1$ in $\mathfrak{L}$, as required.

THEOREM 6.8. *If $S$ is the set of real numbers $0 \leqq x \leqq l$, $(l < \infty)$, under ordinary Lebesgue measure and if $\mathfrak{G}$ is the set of automorphisms of $\mathfrak{L}$ of the form $f(x) \to Tf(\overline{T}x)$ where $T$ is an arbitrary element of $G$ and $\overline{T}$ is an arbitrary measure-preserving transformation of $S$ into itself,*[14] *then $\mathfrak{L}$ is a geometry which is finite and irreducible under $\mathfrak{G}$ as described in §§2, 3, 4, 5, and the normalized dimension function in $\mathfrak{L}$, according to §3, is given by $D(J) = \dfrac{1}{\mu(S)} \int_S D(f(x))\, d\mu(x)$, for $J = J(f(x))$.*

PROOF. By Theorems 6.3, 6.4, 6.5, 6.6, and 6.7, $\mathfrak{L}$ is partially ordered and complete, continuous, modular and complemented, hence a geometry as described in §2. To see that $\mathfrak{L}$ is irreducible under $\mathfrak{G}$, let $J(f(x))$ be such that $J(Tf(\overline{T}x)) = J(f(x))$, that is, $Tf(\overline{T}x) = f(x)$ for almost all $x$, for every measure-preserving transformation $\overline{T}$ of $S$ into itself, and every $T$ in $G$. Since for any subset $S'$ of $S$ of positive measure there exists an at most countable set $\overline{T}_1, \overline{T}_2, \cdots$ such that $\mu\{S - \sum_r \overline{T}_r S'\} = 0$, and since by Definition 6.1 there exists

[14] More generally, $S$ could be any space with finite measure possessing a group $\bar{G}$ of measure-preserving transformations under which $S$ is ergodic, that is, $\mu\{(S' + \overline{T}(S')) - S'\overline{T}(S')\} = 0$ for all $\overline{T}$ in $\bar{G}$, holds only if $\mu(S) = 0$ or $\mu(S - S') = 0$. That von Neumann's use of Fubini's theorem shows that every locally compact, separable group under its own left-translations is ergodic with respect to its left-invariant measures (giving a quick proof of the uniqueness of Haar's measure) has been pointed out independently by S. Kakutani: Proc. Imp. Acad. Tokyo, Vol. XIV, and by J. v. Neumann and the writer.

for every $n$ an element $a_n$ in $L$ such that $\mu\{E_x[d(f(x), a_n) < 1/n^2]\} > 0$, it follows that for this $a_n$, $\mu\{S - E_x[d(f(x), a_n) < 1/n^2]\} = \mu\{S - \sum_r E_x[d(f(\overline{T}_r x), a_n) < 1/n^2]\} = 0$. Hence $f(x) = \sum_{p=1}^{\infty} \prod_{n=p}^{\infty} a_n = a$ say, for almost all $x$. It is clear that $Ta = a$ for every $T$ in $G$. If now $J(f(x))$ is neither 0 nor 1 in $L$, then $a$ is neither 0 nor 1 in $L$, and since $L$ is irreducible under $G$, has at least two different complements in $L$. Let $a_1$, $a_2$ be two such different complements of $a$ in $L$. Set $f_1(x) = a_1$, and $f_2(x) = a_2$ for all $x$. Then clearly $J(f_1(x))$ and $J(f_2(x))$ are two different complements of $J(f(x))$ in $\mathfrak{L}$, showing that $\mathfrak{L}$ is irreducible under $\mathfrak{G}$.

To see that $\mathfrak{L}$ is finite under $\mathfrak{G}$, let $1 = \sum_{\alpha \in I} \oplus J(f_\alpha(x))$, $J(g(x)) = \sum_{\alpha \in I} \oplus J(g_\alpha(x))$, where $J(f_\alpha(x)) \sim J(T_\alpha g(\overline{T}_\alpha x))$ for suitable $T_\alpha$, $\overline{T}_\alpha$. Then Theorem 6.4 implies that $I$ is finite or countable infinite and hence

$$\int_S D(g(x))\, d\mu(x) = \int_S D\left(\sum_n \oplus g_n(x)\right) d\mu(x) = \sum_n \int_S D(g_n(x))\, d\mu(x)$$

$$= \sum_n \int_S D(f_n(x))\, d\mu(x) = \int_S D\left(\sum_n \oplus f_n(x)\right) d\mu(x)$$

$$= \int_S 1\, d\mu(x) = \mu(S).$$

This implies that $D(g(x)) = 1$, and hence that $g(x) = 1$ in $L$, for almost all $x$. Thus if $1 \equiv J(g(x))$ in $\mathfrak{L}$, then $J(g(x)) = 1$ in $\mathfrak{L}$, showing that $\mathfrak{L}$ is finite under $\mathfrak{G}$.

Thus the theory of §§2, 3, 4, 5 applies. Since the dimension function in $\mathfrak{L}$, as defined in §5, is characterized by the properties of being unrestrictedly additive, invariant under the set $\mathfrak{G}$ of automorphisms of $\mathfrak{L}$, and normalized, it follows that it is given by $D(J(f(x)) = \dfrac{1}{\mu(S)} \int_S D(f(x))\, d\mu(x)$.

It is clear that $\mathfrak{L}$, as defined in Definition 6.3, is the smallest geometry with elements which are equivalence classes of functions $f(x)$ (not restricted a priori to be measurable as defined in Definition 6.1) which contains the equivalence classes of the countably valued functions. (If $L$ is a projective geometry, it is easy to show that all equivalence classes in $\mathfrak{L}$ are those of countably valued functions.) The question as to whether there exists a larger set $\mathfrak{L}_1$ of equivalence classes which again form a geometry (necessarily containing $\mathfrak{L}$ as a subgeometry), is open for the general $L$, but has been answered in the affirmative for irreducible geometries $L$ arising from a ring of operators in a Hilbert space, by J. v. Neumann's discovery of such reducible geometries in his study of reducible rings of operators in Hilbert space (unpublished).

HARVARD UNIVERSITY,
CAMBRIDGE, MASSACHUSETTS.

[1]
[2]
[3]
[4]

## BIBLIOGRAPHY

[1] J. v. NEUMANN: Proceedings of the National Academy of Sciences, vol. 32(1938), pp. 92-100, 101-108.

[2] ———: *Lectures on Continuous Geometry*, planographed, Institute for Advanced Study, Princeton, N. J., 1935-37.

[3] ———: *Continuous Geometry*, American Mathematical Society Colloquium Lectures, to appear in book form.

[4] ISRAEL HALPERIN: Transactions of the American Mathematical Society, 44(1938), pp. 537-562.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# THE LATTICE THEORY OF OVA

BY MORGAN WARD AND R. P. DILWORTH[1]

(Received December 21, 1938; revised March 24, 1939)

## I. INTRODUCTION

**1.** In a series of previous papers,[2] we have developed the theory of residuated lattices; that is, lattices over which a multiplication and associated residuation may be defined with the same properties as in polynomial ideal theory. Here we reverse our procedure and start with a system closed under a single suitably restricted operation of multiplication (see section 3). Following E. T. Bell, (Bell 1), we call such a system an "ovum."[3] By the adjunction of properly defined ideals of various kinds (distinguished sub-sets of the ovum), we imbed the ovum in a residuated lattice, incidentally generalizing many of the imbedding theorems of MacNeille 1. The Noether lattices introduced in W-D enables us to describe concisely the arithmetical behavior of ova. In particular, the recent results of A. H. Clifford in these Annals (Clifford 1) come under our general theory. An interesting new result is the following "fundamental theorem of the arithmetic of finite ova." *By the adjunction of a finite number of ideals, every finite ovum may be imbedded in a residuated lattice in which every element, and in particular the elements of the ovum, may be uniquely represented as a cross-cut of primary elements.*

**2.** The plan of this paper is as follows. After some set-theoretic preliminaries, we define and discuss in the third and fourth divisions of the paper two types of distinguished subsets of an ovum, its product ideals and ovoid ideals. (The reader is referred to the paper Clifford 2 in these Annals for the literature and history of ovoid ideals.) In the concluding division of the paper, we give the arithmetical theory of ovoid ideals, obtaining the following general result: *If the lattice of ovoid ideals is modular and if the ascending chain axiom holds, then all of the decomposition theorems of Emmy Noether for the ideals of commutative rings hold.*

**3.** We shall use the lattice terminology of our previous papers. If $\mathfrak{S}$ is a lattice of elements $A, B, \cdots$ and unit element $E$ over which a multiplication is

[1] Portions of this paper have been revised in accordance with suggestions of Dr. A. H. Clifford, who kindly read it in manuscript.

[2] The papers relevant to the present investigation are Ward 1, 2 and the joint paper Ward-Dilworth 1, which we cite here as W-D.

[3] Bell does not postulate the existence of a unit in his general definition.

Other terms are "commutative groupoid" (G. Birkhoff 2), "semi-group" A. H. Clifford 2. For a recent discussion of finite ova, see Poole 1.

defined (Ward 1), we write $X \supset Y$, $Y \subset X$ for $X$ contains $Y$ and $(X, Y)$, $[X, Y]$, $XY$ or $X \cdot Y$ for the union, cross-cut and product respectively of the elements $X$ and $Y$.

Assume that $\mathfrak{S}$ is completely closed relative to union; that is, every subset of elements of $\mathfrak{S}$ has a union. Then if for every subset $\Omega$ of elements $A$ of $\mathfrak{S}$ and any fixed element $B$, the union of the set of elements $BA$ is the product of $B$ and the union of the $A$, we say that multiplication is "completely distributive" relative to union. It is easily shown that multiplication is completely distributive relative to union if and only if the union of the products of all pairs of elements of any two sets of $\mathfrak{S}$ is the product of the unions of the sets.[4] Complete distributivity is of importance because of the following theorem.

THEOREM 3.1. *Let $\mathfrak{S}$ be a lattice which is completely closed relative to union over which a commutative and associative multiplication may be defined distributive with respect to union, and let the unit element of the lattice also be the unit with respect to multiplication. Then a necessary and sufficient condition that any two elements of $\mathfrak{S}$ may have a residual is that multiplication be completely distributive relative to union.*

PROOF. The sufficiency of the condition is established in Ward 1. To prove the necessity, assume that every two elements of $\mathfrak{S}$ have a residual: specifically, given $A$ and $B$, there exists an element $R = A:B$ such that $A \supset RB$; $A \supset XB$ implies $R \supset X$. It is shown in Ward 1 how the ordinary properties of the residual then follow and in particular,

(i) $A:BC = (A:B):C$ (ii) $A \supset B$ if and only if $A:B = E$.

Now let $\Omega$ be any set of elements $A$ of $\mathfrak{S}$, and $B$, a fixed element of $\mathfrak{S}$. Let $U$ and $V$ denote respectively the union of all $A$ and of all $BA$. It suffices to show that $V = BU$. Since $U \supset A$, $BU \supset BA$ for $A \in \Omega$ (Ward 1). Hence $BU \supset V$. But $V \supset BA$, $A \in \Omega$. Hence by (ii) and (i), $E = V:BA = (V:B):A$ or $V:B \supset A$. Hence $V:B \supset U$ or $V \supset BU$, $V = BU$.

4. We understand by an "ovum" a set $O$ of elements $a, b, c, \cdots$ over which a binary relation $x = y$ called "equality" and a binary operation $xy$ called multiplication are well-defined subject to the following conditions: (i) Equality is an equivalence relation; (ii) $O$ is closed under multiplication and multiplication is associative and commutative; (iii) $O$ contains a unit $e$ such that $ae = ea = a$, any $a$ in $O$; (iv) If $a = b$, then $ac = bc$, $ca = cb$ any $c$ in $O$. In short, an ovum is a system satisfying all the usual postulates for an Abelian group save the existence of inverses.[5]

[4] MacNeille 1 has an example showing that complete closure relative to union and distributivity of multiplication relative to union for finite sets does not imply complete distributivity.

[5] The unit $e$ may be dispensed with by strengthening slightly the conditions on the residual introduced later. The non-commutative case will be treated by R. P. Dilworth elsewhere.

For example, any lattice over which a multiplication is defined with the properties in Ward 1 is an ovum with respect to the multiplication whose unit element is the unit of the lattice.

If $U$ and $V$ are subsets of $O$, we denote by $U + V$ and $U \cap V$ their set-theoretic union and cross-cut. Here as usual if $U$ and $V$ have no elements in common, $U \cap V$ is the set-theoretic null class $Z$ containing no elements of $O$ but contained in every other subset.

If $u$ lies in $U$, we write $u \in U$. If $\Omega$ is any class of subsets $A$ of $O$, we write $\sum A$ for the set-theoretic union of the $A$ in $\Omega$. $U \supset V$, $V \subset U$ and $U = V$ denote set-theoretic inclusion and equality.

If $U$ and $V$ are any two subsets, their *set product* $UV$ is by definition the set of all products $uv$, $u \in U$ and $v \in V$. If $U$ consists of a single element $u$, we write $uV$ for $UV$. It is clear that the subsets of $O$ form an ovum with respect to the operation of multiplication so defined, and if $A \supset B$, then $AC \supset BC$ for any $C$. The following theorem is a direct consequence.

THEOREM 4.1. *The operation of multiplication of subsets is completely distributive with respect to set theoretic union.*

In particular $C(A + B) = CA + CB$ for any three sets $A$, $B$ and $C$. On the other hand, $C(A \cap B) \neq CA \cap CB$ in general.

A set $H$ is called a sub-ovum of $O$ if $H^2 \subset H$. A sub-ovum is called "proper" if it contains the unit element $e$ of $O$ and the zero element $z$ whenever the latter exists. Here $z$ is defined by the property $az = z$ for every $a$ of $O$.

Let $\bar{O}$ be a proper sub-ovum of $O$, fixed throughout all that follows. An element $a$ of $O$ is said to "divide" an element $b$ of $O$ (relative to $\bar{O}$) if there exists an element $c$ of $\bar{O}$ such that $ac = b$. We write $a \mid b$. If $a \mid b$ and $b \mid a$, $a$ and $b$ are said to be equivalent (relative to $\bar{O}$); we write then $a \backsim b$. The division relation $\mid$ partially orders $O$, and $\backsim$ is an equivalence relation. Moreover $e \mid a$ for every element $a$ of $\bar{O}$, and if $z$ exists, $a \mid z$ for every $a$ of $O$.

## II. THE PRODUCT IDEALS OF AN OVUM

**5.** The first type of distinguished subset of $O$ which we shall consider is the product ideal.

DEFINITION 5.1. *A subset $S'$ is called a product ideal (relative to $\bar{O}$) if $\bar{O}S' = S'$.*

If in addition $\bar{O} \supset S'$, $S'$ is said to be integral. Clearly $O$ itself is a product ideal. Hence given any subset $A$ of $O$, there is a least product ideal $A'$ containing it. We call $A'$ the ideal generated by $A$. If $A$ consists of a single element $a$, we write $A' = (a)$.

If the ovum contains a zero element $z$, then $z \in S'$ every $S'$ and the ideal $(z)$ is the set $Z$ consisting of $z$ alone. Hence $S' \supset Z$ for every product ideal $S'$. If $O$ contains no zero element, we count the null set $Z$ as a product ideal. It is easily seen that the product ideals of $O(\bar{O})$ are closed under the operations of set-theoretic cross-cut and union.

We denote the union and cross-cut of a set $\Omega$ by $\mu\Omega$ and $\kappa\Omega$ respectively. The following theorem is now evident:

THEOREM 5.1. *The set of all product ideals and the set of all integral product ideals of any ovum both form distributive lattices which are completely closed with respect to union and cross-cut.*

THEOREM 5.2. *The set of all integral product ideals of an ovum form a residuated lattice completely closed relative to union and cross-cut.*

PROOF. Since the union and cross-cut operations on ideals in $\bar{O}$ are the set-theoretic operations on the ideals qua classes of elements, it is evident that the ideals form a completely closed distributive lattice. The postulates for a multiplication in a lattice are

M 1 *If $\bar{O}$ contains $A'$, $B'$, then $\bar{O}$ contains $A'B'$.*

M 2 *If $A' = B'$, then $A'C' = B'C'$.*

M 3 $A'B' = B'A'$.

M 4 $(A'B')C' = A'(B'C')$.

M 5 $A'O' = A'$ any $A'$. (Here $O' = \bar{O}$).

M 6 $A'(B', C') = (A'B', A'C')$.

These postulates are clearly all satisfied. We shall denote this lattice by $\mathfrak{R}$. We also have from theorems 3.1 and 4.1

M 7 *$\mathfrak{R}$ is completely closed with respect to union, and the product of the unions of any two classes of ideals of $\mathfrak{R}$ is the union of the set-products of all pairs of elements in the classes.*

Hence (Ward 1) a residuation $X':Y'$ may be defined over $\mathfrak{R}$ with the properties R 1–R 6 given in W-D, §4, so that the ideals of $\bar{O}$ form a residuated lattice by definition.

It is impossible to prove that the lattice of *all* product ideals of $O$ may be residuated, for the unit element $O$ of the lattice is not the unit with respect to multiplication, so that M 5 is not satisfied. All the remaining postulates are satisfied. A similar situation occurs in defining the product of two modules of a ring of algebraic integers (Dedekind 1). M 5 is arithmetically important, as it assures that $A' \supset A'B'$.

If $a$ is any element of $\bar{O}$, the product ideal $(a)$ is clearly the set $a\bar{O}$ of all multiples of $a$ in $\bar{O}$. We call $(a)$ an (integral) principal ideal.

THEOREM 5.3. *If $A'$ is an integral principal ideal and $A' \supset B'$, then there exists an integral ideal $C'$ such that $A'C' = B'$.*

PROOF. By hypothesis, $A' = a\bar{O}$. Since $A' \supset B'$, every element of $B'$ is of the form $aq$, where $q$ lies in a certain fixed class $Q$ of $\bar{O}$. Then

$$B' = \sum_Q aq\bar{O} = \sum a\bar{O}q\bar{O} = a\bar{O}\sum q\bar{O} = A'C'$$

where $C'$ is the ideal $\sum q\bar{O}$.

It follows from M 7 in the proof of theorem 5.5, and W-D, lemma 13.1, that we may take $C' = B':A'$.[6]

[6] There may be several ideals $C'$ such that $A'C' = B'$.

**6.** It may be shown by simple examples that if the ovum $\bar{O}$ contains an infinite number of non-equivalent elements, no chain conditions need be satisfied in $\mathfrak{R}$, or in other words integral product ideals are in general expressible only as unions of an infinite number of elements of $\bar{O}$. If however $\bar{O}$ contains only a finite number of non-equivalent elements, then $\mathfrak{R}$ is a finite lattice satisfying the following conditions:[7]

N 1. *$\mathfrak{R}$ is residuated.*

N 2. *The ascending chain condition holds in $\mathfrak{R}$.*

D 3. *Every element of $\mathfrak{R}$ is the union of a finite number of principal ideals.*

D 4. *The principal ideals of $\mathfrak{R}$ are closed under multiplication.*

Hence by theorem 5.3 and theorem 14.2 of W-D, $\mathfrak{R}$ is a Noether lattice. Since $\mathfrak{R}$ is also a distributive lattice, we may state the following theorem.

THEOREM 6.1. *If $\bar{O}$ contains only a finite number of principal product ideals, then every element of $\bar{O}$ is expressible as a cross-cut of a finite number of primary product ideals in essentially one way only.*

If in particular $O$ itself has only a finite number of elements, and we take $\bar{O} = O$, we have the "fundamental theorem of the arithmetic of finite ova" stated in the introduction.

## III. THE OVOID IDEALS OF AN OVUM

**7.** The second type of distinguished subset of $O$ which we shall consider is the ovoid ideal. There is little gain in defining division in $O$ relative to a proper subovum $\bar{O}$, and for the remainder of the paper we identify $\bar{O}$ with $O$ as in Clifford 2.

DEFINITION 7.1. *Let $A$ be any set of elements of $O$. The cross-cut of all the residuals $(s):(t)$ of principal product ideals $(s)$, $(t)$ such that $(s):(t)$ contains $A$ is called the ovoid ideal generated by $A$.*

We write $\mathfrak{a} = (A)$ (Clifford 2). Evidently $\mathfrak{a}$ is a product ideal containing both $A$ and $A'$. It is easily shown that this definition is equivalent to the definition in Clifford 2. It seems to us somewhat easier to grasp.

$O$ itself is an ovoid ideal $\mathfrak{o}$, and the ovoid ideals form a semi-ordered set with respect to the relation $(\mathfrak{x}) \supset (\mathfrak{y})$ of set-theoretic inclusion. We use small German letters for ovoid ideals.

As in part II, a special convention is made for the null ideal. If the ovum contains a zero element $z$, the set $\mathfrak{z}$ consisting of the single element $z$ is an ovoid ideal contained in every other ideal. If the ovum contains no zero element, we count the null set as an ovoid ideal $\mathfrak{z}$ contained in every other.

The following properties of ovoid ideals are obvious from the definition:

(7.1) $\quad (A) \supset A, \quad A \supset B \quad$ implies $\quad (A) \supset (B), \quad ((A)) = (A).$

LEMMA 7.1. (Clifford 2) *If the subset $A$ consists of a single element $a$, the ovoid ideal $(A)$ is the principal product ideal $(a) = aO$.*

[7] The letters N 1, N 2, D 3, D 4 refer to the like-designated conditions in W-D.

THEOREM 7.1. *The set-theoretic cross-cut of any class of ovoid ideals is an ovoid ideal.*

PROOF. Let $\Omega$ be a class of ovoid ideals $\mathfrak{a}$, and let $K$ be the set-theoretic cross-cut of the $\mathfrak{a}$. ($K$ exists, since $\mathfrak{a} \supset \mathfrak{z}$). Then $\mathfrak{a} \in \Omega$ implies $\mathfrak{a} \supset K$. Hence by (7.1), $(\mathfrak{a}) \supset (K)$, $\mathfrak{a} \supset (K)$. Hence $K \supset (K)$, $K = (K)$.

We may now define the union of any set of ovoid ideals $\mathfrak{b}$ as the cross-cut of the non-empty set $\Omega$ of all ideals $\mathfrak{a}$ such that $\mathfrak{b} \supset \mathfrak{a}$, all $\mathfrak{b}$. It is easy to prove from (7.1):

LEMMA 7.2. (Clifford 2) *The union of any set of ovoid ideals is the ovoid ideal generated by their set theoretic sum.*

We may now state one of our fundamental theorems.

THEOREM 7.2. *The set of ovoid ideals of any ovum form a completely closed lattice relative to the relation of set-theoretic inclusion.*

8. We now pass to the multiplicative properties of the lattice of ovoid ideals. The set product of two ovoid ideals need not be an ovoid ideal. We accordingly define the product of two ovoid ideals to be the ideal generated by their set product. To distinguish this new product from the set product, we use a dot, writing

$$(A)\cdot(B) = ((A)(B)), \quad \text{or} \quad \mathfrak{a}\cdot\mathfrak{b} = (\mathfrak{a}\mathfrak{b}). \tag{8.1}$$

This multiplication is readily shown to satisfy postulates M 1–M 5 of section 5, where the unit element is the unit ideal $\mathfrak{o}$.

THEOREM 8.1. *The operation of multiplication of ovoid ideals is completely distributive with respect to union.*

PROOF. Let $\Omega$ be any set of ovoid ideals $\mathfrak{a}$, and let $\mathfrak{b}$ be any fixed ovoid ideal. Let $\mathfrak{u}$ be the union of the ideals $\mathfrak{a}$, and $\mathfrak{v}$ the union of the ideals $\mathfrak{b}\cdot\mathfrak{a}$. Then by lemma 7.2 $\mathfrak{u} = (\sum \mathfrak{a})$, $\mathfrak{v} = (\sum \mathfrak{b}\cdot\mathfrak{a})$. We wish to show that $\mathfrak{b}\cdot\mathfrak{u} = \mathfrak{v}$. We need the following lemma due to A. H. Clifford: (Clifford 2).

LEMMA 8.1. *If $A$ and $B$ are any two subsets of $O$, then the product of the ovoid ideals which they generate is the ideal generated by their set product:*

$$(A)\cdot(B) = (AB). \tag{8.2}$$

By (8.2), $\mathfrak{b}\cdot\mathfrak{u} = (\mathfrak{b}\sum \mathfrak{a}) = (\sum \mathfrak{b}\mathfrak{a})$ by theorem 4.1. But by lemma 7.2 $(\sum \mathfrak{b}\mathfrak{a}) = (\sum (\mathfrak{b}\mathfrak{a})) = (\sum \mathfrak{b}\cdot\mathfrak{a}) = \mathfrak{v}$

It follows that M 7 and M 6 of section 5 are satisfied. Hence we have

THEOREM 8.2. *The set of all ovoid ideals of $O$ form a completely closed residuated lattice.*

We denote this lattice by $\mathfrak{S}$.

If $(a)$ and $(b)$ are principal ovoid ideals, it is easily shown that $(a)\cdot(b) = (a)(b) = (ab)$. Hence we have

LEMMA 8.2. *The principal ovoid ideals of $O$ are closed under multiplication, and form an ovum within the lattice $\mathfrak{S}$ which is simply isomorphic with $O$.*

In W-D, an element $\mathfrak{a}$ of a residuated lattice $\mathfrak{S}$ was defined to be "principal" provided that $\mathfrak{a} \supset \mathfrak{b}$ if and only if there existed a lattice element $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$.

THEOREM 8.3. *Every principal ideal of the lattice of all ovoid ideals of an ovum is a principal element of the lattice.*

PROOF. Let $\mathfrak{a} = (a)$ and $\mathfrak{a} \supset \mathfrak{b}$. Consider the set $C$ of all elements $c$ such that $ac \in \mathfrak{b}$ and let $\mathfrak{c} = (C)$. Then $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$. For since $\mathfrak{b} \supset aC$, $(\mathfrak{b}) \supset (aC)$ or $\mathfrak{b} \supset \mathfrak{a} \cdot \mathfrak{c}$. Since $\mathfrak{a} \supset \mathfrak{b}$ and $\mathfrak{a} = (a)$, if $b \in \mathfrak{b}$ then $b = ca$, $c \in O$. Hence $aC \supset \mathfrak{b}$ so that $(aC) \supset \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{c} \supset \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}$.

## IV. THE ARITHMETICAL PROPERTIES OF OVA

**9.** We shall now consider the arithmetical properties of the lattice $\mathfrak{S}$. In W-D, we have called a lattice a "Noether lattice" if it satisfies the three conditions.

N 1. *The lattice $\mathfrak{S}$ may be residuated.*

N 2. *The ascending chain condition holds in $\mathfrak{S}$.*

N 3. *Every irreducible of $\mathfrak{S}$ is primary.*

In such a lattice the decomposition theorems first proved by Emmy Noether for the ideals of a commutative ring with chain condition hold. We also proved there that sufficient conditions[8] that any lattice be a Noether lattice are N 1, N 2 and

D 2 *$\mathfrak{S}$ is modular.*

D 3′ *There exists a set $\mathfrak{P}$ of principal elements of $\mathfrak{S}$ such that every other element is the union of a finite number of elements of $\mathfrak{P}$.*

D 4′ *The set $\mathfrak{P}$ is closed under multiplication.*

In the present case, N 1 is satisfied by theorem 8.2, and D 4′ is satisfied for $\mathfrak{P}$ the principal ideals of $\mathfrak{S}$ by lemma 8.2. Clifford has shown that N 2 implies D 3′ (Theorem 8.4; Clifford 2, theorem 2.1). Hence we may state the fundamental result:

THEOREM 9.1. *The lattice of ovoid ideals of any ovum is a Noether lattice provided that*

N 2. *The ascending chain condition holds in $\mathfrak{S}$,*

D 2. *$\mathfrak{S}$ is modular.*

If we assume that $\mathfrak{S}$ is distributive instead of modular, we have an analogue of theorem 6.1 on product ideals; namely

THEOREM 9.2. *If the lattice of ovoid ideals of an ovum satisfies the conditions*

N 2. *The ascending chain condition holds in $\mathfrak{S}$,*

D 6. *$\mathfrak{S}$ is distributive,*

*then every element of the lattice, and in particular the principal ideals corresponding*

---

[8] The more restrictive conditions D 3 and D 4 quoted in section 6 are stated in W-D. But an examination of the proof of theorem 14.2 of W-D will show that D3′ and D4′ are sufficient.

*to elements of the ovum, may be uniquely represented as a cross-cut of primary elements, each belonging to a different prime.*

If we assume that every ovoid ideal is principal, then D 6 is satisfied by W-D theorem 16.2. Hence we may state:

THEOREM 9.3. *The conclusions of theorem* 9.2 *hold provided that the lattice of ovoid ideals satisfies the conditions*

N 2. *The ascending chain condition holds in* $\mathfrak{S}$,

D 7. *Every ovoid ideal is principal.*

**10.** The two simplest types of distributive lattice are arithmetical lattices and semi-arithmetical lattices. An arithmetical lattice is one which is a direct product[9] of simple chain lattices and in which N 2 holds. It is quite easy to show that the fundamental theorem of arithmetic[10] holds in a lattice if and only if the lattice is arithmetical. Such lattices have been thoroughly investigated by F. Klein (Klein 1).

The notion of a semi-arithmetical lattice was introduced by one of us in a recent paper in these Annals. (Ward 2.) A semi-arithmetical lattice is a distributive lattice in which the ascending chain condition holds and in which every element may be uniquely represented as a cross-cut of irreducible elements *co-prime in pairs*. If the semi-arithmetical lattice is residuated, it follows that every element may be uniquely represented as a *product* of irreducible elements; for if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, their product equals their cross-cut. Conversely, it is not difficult to show that if every element of a lattice may be uniquely represented as a product of irreducible elements, co-prime in pairs, then the lattice is semi-arithmetical; in other words a residuated semi-arithmetical lattice is the most general type of lattice in which a unique multiplicative decomposition of elements may be defined.

We can therefore replace condition D 6 by conditions that $\mathfrak{S}$ be semi-arithmetical or arithmetical to obtain still more special types of decomposition in $\mathfrak{S}$. The investigations of Clifford viewed from this standpoint give convenient sets of conditions that the lattice be arithmetical.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA.

## REFERENCES

E. T. BELL 1 Am. Math. Monthly 37 (1930) pp. 400–418.
GARRETT BIRKHOFF 1 Bull. Am. Math. Soc. 40 (1934) pp. 613–619.
2 These Annals (2) 35 (1934) pp. 351–360.
A. H. CLIFFORD 1 Bull. Am. Math. Soc. 40 (1934) pp. 326–330.
2 These Annals (2) 39 (1938) pp. 594–610.

[9] For the notion of a direct product of lattices, see Garrett Birkhoff 1.

[10] Every lattice element is then uniquely representable as a cross-cut or product of co-prime powers of divisor free elements. (Klein 1.)

| | | |
|---|---|---|
| R. DEDEKIND | 1 | Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed. |
| L. E. DICKSON | 1 | Trans. Am. Math. Soc. 6 (1905) p. 205. |
| F. KLEIN | 1 | Math. Annalen 106 (1932) pp. 114–134. |
| H. M. MACNEILLE | 1 | Trans. Am. Math. Soc. 42 (1937) pp. 416–460. |
| A. R. POOLE | 1 | Am. Math. Journ. 59 (1937) pp. 23–32. |
| M. WARD AND R. P. DILWORTH | | Trans. Am. Math. Soc. (reference later). |
| M. WARD | 1 | Duke Math. Journ. 3 (1937) pp. 627–636. |
| | 2 | These Annals (2) 39 (1938) pp. 558–568. |

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# A CHARACTERIZATION OF BOOLEAN ALGEBRAS

BY GARRETT BIRKHOFF AND MORGAN WARD

(Received January 9, 1939)

## Introduction

When is a lattice a Boolean algebra—that is, isomorphic with a field of sets? The classical conditions are:[1] (1) The distributive law holds, (2) every element has a complement. Now it is well known[2] that (1) and (2) imply (3) no element has more than one complement. We are thus led to conjecture that (2) *and* (3) *imply* (1); in other words, that a necessary and sufficient condition that a lattice be a Boolean algebra is that each of its elements have a unique complement.

The only published result bearing on this question is G. Bergmann's[3] theorem that the distributive law holds if and only if *relative* complements are unique; that is, if and only if given $a \leqq x \leqq b$, there exists one and only one $y$ with $x \cap y = a$, $x \cup y = b$.

We prove here the truth of our conjecture for all complete atomistic lattices.[4] These include lattices of finite length and of finite order. We do not know whether or not our conjecture is unrestrictedly true.

## Exact statement of theorem

Let $L$ be a complete lattice which is "atomistic" in the sense that if $O < a < I$, then $p_\alpha \leqq a \leqq q_\beta$ where $p_\alpha$ covers $O$ and $q_\beta$ is covered by $I$. Let us further define a "point" as an element $p$ covering $O$.

THEOREM 1: *If each element of $L$ has one and only one complement, then $L$ is isomorphic with the Boolean algebra of all subsets of its points.*

THEOREM 2: *In order for $L$ to be a Boolean algebra, it is necessary and sufficient that each element have one and only one complement.*

The second theorem follows from the first, and the known results stated in the introduction.

PROOF OF FIRST THEOREM. To each set $S$ of points $p_\alpha$, make correspond the join $x(S)$ of the $p_\alpha$ in $S$. Dually, associate with each set $S$ of elements $q_\beta$ covered by $I$, the meet $y(S)$ of the $q_\beta$ in $S$. It will follow from generalized

[1] E. V. Huntington "Postulates for the algebra of logic," Trans. Am. Math. Soc. 5 (1904), pp. 288–309. His hypotheses (1) — (7) define lattices.

[2] See for example, A. N. Whitehead's "Universal Algebra" Cambridge (1898) p. 36. The result is due to R. Grassmann.

[3] "Zur Axiomatik der Elementargeometrie" Monatschr. f. Math. u. Phys. 36 (1929), pp. 269–84.

[4] The terminology of the present paper is that of G. Birkhoff's "Lattice theory and its applications" Bull. Am. Math. Soc. 44 (1938), pp. 793–800. By "$a$ covers $b$," we mean that $a > b$ while $a > x > b$ has no solution.

associativity, that $x(S \cup T) = x(S) \cup x(T)$ and $y(S \cup T) = y(S) \cap y(T)$. Again, the complement of $x(I)$ can contain no point, since $x(I)$ contains every point;[5] hence it is $O$, and $x(I) = I$. Dually, $y(I) = O$.[5]

Again, given $\alpha$, $\beta$, either $p_\alpha \leqq q_\beta$, or $p_\alpha \cap q_\beta = O$ and $p_\alpha \cup q_\beta = I$—that is, $p_\alpha$ and $q_\beta$ are complementary. But not every $q_\beta$ contains $p_\alpha$, since $y(I) = O < p_\alpha$. Hence (by the existence of unique complements) a suitable subscript notation will make $p'_\alpha = q_\alpha$ and $p_\alpha \leqq q_\beta$ if $\alpha \neq \beta$.

This notation will further identify subsets of $p_\alpha$ with subsets of $q_\alpha$, and, since every $p_\alpha$ $[\alpha \in S]$ is less than or equal to every $q_\beta$ $[\beta \in S']$, it will make $x(S) \leqq y(S')$. (Here $S'$ denotes the set complementary to $S$.) From this important inequality we infer that

$$x(S) \cup y(S) \geqq x(S) \cup x(S') = x(S \cup S') = I,$$

$$x(S) \cap y(S) \leqq y(S') \cap y(S) = y(S \cup S') = O.$$

Consequently $x(S)$ and $y(S)$ are complementary.

Also, $x(S) \cap x(S') \leqq y(S') \cap y(S) = y(S \cup S') = O$ and $x(S) \cup x(S') = x(S \cup S') = I$; hence $x(S)$ and $x(S')$ are complementary. But since $x(S)$ and $x(S')$ are complementary, $x(S)$ contains no $p_\alpha$ not in $S$, distinct sets $S$ determine distinct $x(S)$, and the partially ordered system of the $x(S)$ is isomorphic with the algebra of all subsets of the $p_\alpha$.

It remains to show that every member $a$ of $L$ is an $x(S)$. But denote by $S$ the set of $p_\alpha \leqq a$. Evidently $x(S) \leqq a$; moreover $a \cap x(S')$ will by the last paragraph contain no points; hence $a \cap x(S') = O$. On the other hand, $a \cup x(S') \geqq x(S) \cup x(S') = I$; hence $a$ is the unique complement $x(S)$ of $x(S')$, completing the proof.

HARVARD UNIVERSITY AND
CALIFORNIA INSTITUTE OF TECHNOLOGY.

[5] We are letting $I$ denote simultaneously: the biggest element in $L$, the set of all $p_\alpha$, and the set of all $q_\beta$.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ON FROBENIUSEAN ALGEBRAS. I[1]

BY TADASI NAKAYAMA

(Received February 2, 1939)

## Introduction

Let $A$ be an algebra possessing a unit element. Let $R(a)$ and $S(a)$ $(a \in A)$ be the right (first) and the left (second) regular representations of $A$ (defined by a certain basis). $A$ is called *Frobeniusean* if $R(a)$ and $S(a)$ are equivalent to each other, while we call $A$ *quasi-Frobeniusean* if the totality of distinct directly indecomposable components of $R(a)$ coincides with that of $S(a)$. Furthermore, $A$ is called *symmetric* if $R(a)$ can be transformed into $S(a)$ by a symmetric non-singular matrix; the notion was introduced by R. Brauer and C. Nesbitt.[2] The present note studies the structure of these and some other related types of algebras.

Section 1 is a preliminary and is a restatement of the known structural theory of algebras together with its bearings on the representation theory. Then in the succeeding three sections we prove the main theorems on Frobeniusean and quasi-Frobeniusean algebras which state: an algebra $A$ over a field $F$ is Frobeniusean if and only if $\alpha)$ $l(r(\mathfrak{l})) = \mathfrak{l}$, $r(l(\mathfrak{r})) = \mathfrak{r}$ and $\beta)$ $(\mathfrak{l}:F) + (r(\mathfrak{l}):F) = (A:F)$, $(\mathfrak{r}:F) + (l(\mathfrak{r}):F) = (A:F)$ for every left ideal $\mathfrak{l}$ and right ideal $\mathfrak{r}$ (Th. 1), while $A$ is quasi-Frobeniusean if and only if $\alpha)$ (but not necessarily $\beta)$) holds for every $\mathfrak{l}$ and $\mathfrak{r}$ (Th. 2); where $r(S)$ $[l(S)]$, with a set $S$ of elements in $A$, denotes the set of all right [left] annihilators of $S$ in $A$. In fact, as for the first parts (that is, the "if" parts) of the assertions we have only to assume the validity of the relations for every nilpotent simple left ideal and nilpotent simple right ideal as well as for the radical and the zero ideal (Th. 3). Section 5 deals with some immediate consequences and supplementaries of the above theorems. For instance, we show that if $A$ is quasi-Frobeniusean and $N$ is the radical of $A$ then $r(N^\nu) = l(N^\nu)$ for any $\nu$ (Th. 6), and that if a two-sided ideal $\mathfrak{z}$ of a Frobeniusean algebra $A$ is a principal left ideal $\mathfrak{z} = Ac$, then $\mathfrak{z} = cA$, too, and conversely (Th. 4, Corollary). In 6 we examine under what condition a residue class algebra of a Frobeniusean algebra would be again Frobeniusean; the answer is that $A/\mathfrak{z}$, where $A$ is Frobeniusean and $\mathfrak{z}$ is a two-sided ideal in $A$, is Frobeniusean if and only if the two-sided ideal $r(\mathfrak{z})$ is principal $r(\mathfrak{z}) = Ac = cA$ (Th. 9). As an application we then obtain, in 7, a characterization of such an algebra $A$ in which every two-sided ideal is expressible as $\mathfrak{z} = Ac = cA$ (Th. 10).

[1] Presented to the American Mathematical Society on Sept. 6, 1938 and Feb. 29, 1939 in parts.

[2] Brauer-Nesbitt (3), Nesbitt (13), (14). Cf. also Nakayama-Nesbitt (11).

The last two sections are devoted mainly to symmetric algebras. Namely, 8 studies, as a preliminary, the relationship between left and right representation moduli[3] belonging to mutually equivalent representations of an algebra, which is in fact essentially nothing but the well known relationship between so-called dual vector spaces.[4] Then in 9 we show that in case of a symmetric algebra the 1-1 dual correspondence of left and right ideals by annihilation, which was established in the above Theorem 1, is in accord with the representation theory, that is, if $A$ is a symmetric algebra and if $\mathfrak{l}_0$ is a left subideal of a left ideal $\mathfrak{l}$ in $A$, the representation of $A$ defined by the left module $\mathfrak{l}/\mathfrak{l}_0$ is equivalent to the one defined by the right module $r(\mathfrak{l}_0)/r(\mathfrak{l})$ (Th. 12). We obtain also a necessary and sufficient condition that a residue class algebra of a symmetric algebra be symmetric (Th. 13). Finally, in an appendix at the end we re-formulate and generalize a fundamental theorem on parastrophic matrices[5] which is a starting point of our study.

In Part II, which will come later, we shall mainly deal with general rings satisfying chain conditions for ideals and shall see that most of those results in the present part which are concerned with Frobeniusean and quasi-Frobeniusean algebras can be extended to that general case if we define the corresponding types of rings in a suitable manner.[6]

The writer is grateful to Prof. R. Brauer and Dr. C. Nesbitt, to whom the present paper owes very much. Furthermore, an impulse was given to the present paper by a seminar directed by Prof. H. Weyl, as well as by a recent work of Dr. M. Hall.[7]

## 1. Preliminaries[8]

Let $A$ be an (associative) algebra (with a finite basis) over a field $F$, and let $N$ be the radical of $A$. We assume $N \neq A$. The residue class algebra $\bar{A} = A/N$ is semisimple and is a direct sum of simple[9] two-sided ideals which themselves are simple algebras,

$$\bar{A} = \bar{A}_1 + \bar{A}_2 + \cdots + \bar{A}_k .$$

Let $\bar{E}_1, \bar{E}_2, \cdots, \bar{E}_k$ be the unit elements of $\bar{A}_1, \bar{A}_2, \cdots, \bar{A}_k$. Each $\bar{E}_\kappa$ can be decomposed into a sum of mutually orthogonal idempotent elements $\bar{e}_{\kappa,1}$, $\bar{e}_{\kappa,2}, \cdots, \bar{e}_{\kappa,f(\kappa)}$ such that left ideals $\bar{A}\bar{e}_{\kappa,i}$ as well as right ideals $\bar{e}_{\kappa,i}\bar{A}$ are simple.

[3] We shall call a representation module of an algebra a left or right one according as the algebra is a left or a right operator domain.

[4] Weyl (17), Chap. I, §3.

[5] Frobenius (6). See also the papers referred to in the footnote 2.

[6] For instance, we may use the properties of the criteria in Lemma 2 (Section 2) to define Frobeniusean and quasi-Frobeniusean rings.

[7] Hall (7).

[8] See Artin (1), Deuring (5), Köthe (8), Noether (15). Cf. also Brauer-Nesbitt (3), Nakayama (10).

[9] By a simple two-sided [left, right] ideal we shall always mean a *non-zero* simple two-sided [left, right] ideal.

There exists a system of mutually orthogonal idempotent elements $e_{\kappa,i}$ in $A$ such that $e_{\kappa,i} \pmod N = \bar{e}_{\kappa,i}$ $(\kappa = 1, 2, \cdots, k;\ i = 1, 2, \cdots, f(\kappa))$. Put $E_\kappa = \sum_{i=1}^{f(\kappa)} e_{\kappa,i}$ and $E = \sum_\kappa E_\kappa$. $A$ is a direct sum

$$\begin{aligned} A &= Ae_{1,1} + \cdots + Ae_{1,f(1)} + Ae_{2,1} + \cdots + Ae_{k,f(k)} + \mathfrak{l}_0, \\ [A &= e_{1,1}A + \cdots + e_{1,f(1)}A + e_{2,1}A + \cdots + e_{k,f(k)}A + \mathfrak{r}_0], \end{aligned} \tag{1}$$

where $\mathfrak{l}_0[\mathfrak{r}_0]$ is a left [right] ideal $\subseteq N$ consisting of all left [right] annihilators of $E$. ($\mathfrak{l}_0 = \mathfrak{r}_0 = 0$ if and only if $A$ has a unit element; in this case $E$ is really the unit element.) The idempotent elements $e_{\kappa,i}$ are primitive,[10] and the left ideals $Ae_{\kappa,i}$ as well as the right ideals $e_{\kappa,i}A$ are directly indecomposable. Furthermore

$$Ae_{\kappa,1} \cong Ae_{\kappa,2} \cong \cdots \cong Ae_{\kappa,f(\kappa)}\ [e_{\kappa,1}A \cong e_{\kappa,2}A \cong \cdots \cong e_{\kappa,f(\kappa)}A], \tag{2}$$

and there exists for each $\kappa$ a system of $f(\kappa)^2$ elements $c_{\kappa,ij} (i, j = 1, 2, \cdots, f(\kappa))$ such that $c_{\kappa,ii} = e_{\kappa,i}$, $c_{\kappa,ij}c_{\kappa,kl} = \delta_{jk}c_{\kappa,il}$ (Kronecker $\delta$).

For the sake of brevity let us denote one of $e_{\kappa,i} (i = 1, 2, \cdots, f(\kappa))$, say $e_{\kappa,1}$, by $e_\kappa$. Incidentally we denote $\bar{e}_{\kappa,1}$ by $\bar{e}_\kappa$. $Ne_\kappa = N \cap Ae_\kappa [e_\kappa N = N \cap e_\kappa A]$ is a unique maximal left [right] subideal of $Ae_\kappa [e_\kappa A]$.[11] A simple left [right] module[12] of $A$ is either annihilated by $A$ or is isomorphic to one (and only one) of $\bar{A}\bar{e}_\kappa (\cong Ae_\kappa/Ne_\kappa)$ $[\bar{e}_\kappa\bar{A} (\cong e_\kappa A/e_\kappa N)]$ $(\kappa = 1, 2, \cdots, k)$.

LEMMA 1. *If a left module* $\mathfrak{m}$ *of* $A$ *has a unique maximal submodule* $\mathfrak{m}_1$ *and if* $\mathfrak{m}/\mathfrak{m}_1$ *is isomorphic to* $\bar{A}\bar{e}_\kappa$, *then* $\mathfrak{m}$ *is homomorphic to* $Ae_\kappa$. *If a right representation module* $\mathfrak{n}$ *of* $A$ *has a unique simple submodule* $\mathfrak{n}_0$ *and if* $\mathfrak{n}_0 \cong \bar{e}_\kappa\bar{A}$, *then a representation of* $A$ *belonging to the left ideal* $Ae_\kappa$ *can be reduced to the form*

$$\begin{pmatrix} N(a) & 0 \\ * & * \end{pmatrix}$$

*where* $N(a)$ *belongs to* $\mathfrak{n}$.

PROOF. Denote $e_\kappa$ by $e$. $e\mathfrak{m} \not\subseteq \mathfrak{m}_1$ since $\mathfrak{m}/\mathfrak{m}_1 \cong \bar{A}\bar{e}_\kappa$. Let $u \in e\mathfrak{m}$ but $\notin \mathfrak{m}_1$. Then $Au = \mathfrak{m}$, for $u (= eu \in Au) \notin \mathfrak{m}_1$ and $\mathfrak{m}_1$ is a unique maximal submodule of $\mathfrak{m}$. Hence $ae \to au (a \in A)$ is a homomorphic mapping of $Ae$ onto $\mathfrak{m}$. This proves the first half of the lemma. To prove the second half we have merely to consider, instead of $\mathfrak{n}$, a *left* representation module belonging to $N(a)$ and to apply the first half to it; observe that (irreducible) representations belonging to $\bar{A}\bar{e}_\kappa$ and $\bar{e}_\kappa\bar{A}$ are equivalent.

Now, if $S$ is a set of elements in $A$ we denote by $r(S)$ $[l(S)]$ the set of all right [left] annihilators of $S$ in $A$. $r(S)$ $[l(S)]$ is a right [left] ideal. If in particular $S$ is a right [left] ideal, then $r(S)$ $[l(S)]$ is a *two-sided* ideal.

---

[10] An idempotent element is called primitive if it can not be decomposed into a sum of two mutually orthogonal idempotent elements.

[11] Such is the case for any primitive idempotent element.

[12] By a left [right] module of $A$ we understand as usual an additive group which has $A$ not only as a mere (left [right]) operator domain but as an operator *algebra*. (Thus it has also elements of the underlying field $F$ as operators, and it can be considered as a representation module whenever it has a finite rank over $F$.)

The two-sided ideal $r(N)$, where $N$ is the radical of $A$, is the largest completely reducible left ideal of $A$, that is, the sum of all simple left ideals of $A$. For, if $\mathfrak{l}$ is a simple left ideal then $N\mathfrak{l} = 0$ whence $\mathfrak{l} \subseteq r(N)$, while $r(N)$ is certainly a completely reducible left ideal since $Nr(N) = 0$. Furthermore, for each $\kappa$ $E_\kappa r(N)$ is the sum of all simple left ideals isomorphic to $\bar{A}\bar{e}_\kappa$, as can readily be seen from the fact that a simple left module $\mathfrak{m}$ of $A$ is isomorphic to $\bar{A}\bar{e}_\kappa$ if and only if $E_\kappa\mathfrak{m} = \mathfrak{m}$. Hence $E_\kappa r(N)$ is a two-sided ideal, for if $\mathfrak{l} \cong \bar{A}\bar{e}_\kappa$ then $\mathfrak{l}a (a \in A)$ is either $\cong \bar{A}\bar{e}_\kappa$ or 0. $r(N)$ is the direct sum

$$E_1 r(N) + E_2 r(N) + \cdots + E_k r(N) + (r(N) \cap \mathfrak{r}_0),$$

where $\mathfrak{r}_0 = r(E)$ as in (1); some of $E_\kappa r(N)$ as well as $r(N) \cap \mathfrak{r}_0$ may be 0. Similarly $l(N)$ is the largest completely reducible right ideal and we have its decomposition analogous to above.

It may be also useful to note that if $\mathfrak{l}$ is any left ideal of $A$, $\mathfrak{l} \cap r(N)$ is the largest completely reducible left subideal of $\mathfrak{l}$. In particular, in order that $\mathfrak{l}$ has a unique simple left subideal it is necessary and sufficient that $\mathfrak{l} \cap r(N)$ is simple.

## 2. Frobeniusean and quasi-Frobeniusean algebra

Let $A$ be an algebra over a field $F$ and let $N$, $e_{\kappa,i}$, $e_\kappa (= e_{\kappa,1})$, $E_\kappa$, $E$, $f(\kappa)$, etc. have the same significance as in 1. Let further $S(a)$ and $R(a)$ be the left (second) and the right (first) regular representations of $A$ (defined by a certain basis). If $A$ possesses a unit element, which necessarily coincides with $E$, then $\mathfrak{l}_0$ and $\mathfrak{r}_0$ in (1) are both 0, whence

$$\begin{aligned} A &= Ae_{1,1} + \cdots + Ae_{1,f(1)} + Ae_{2,1} + \cdots + Ae_{k,f(k)} \\ &= e_{1,1}A + \cdots + e_{1,f(1)}A + e_{2,1}A + \cdots + e_{k,f(k)}A, \end{aligned}$$

and this expresses a decomposition of $S(a)$ and $R(a)$ into (directly) indecomposable components. Namely, if $V_\kappa(a)$ and $U_\kappa(a)$ are representations of $A$ belonging to the left ideal $Ae_\kappa$ and the right ideal $e_\kappa A$ respectively, then

$$S(a) \cong \sum_\kappa f(\kappa) \cdot V_\kappa(a), \qquad R(a) \cong \sum_\kappa f(\kappa) \cdot U_\kappa(a). \tag{3}$$

DEFINITION. *$A$ is called Frobeniusean if it possesses a unit element and if $S(a)$ and $R(a)$ are equivalent to each other: $S(a) \cong R(a)$, while we call $A$ quasi-Frobeniusean if it possesses a unit element and if the totality of distinct (= inequivalent) indecomposable components of $S(a)$ coincides with that of $R(a)$, that is, if there exists a permutation $(\pi(1), \pi(2), \cdots, \pi(k))$ of $(1, 2, \cdots, k)$ such that $V_{\pi(\kappa)}(a) \cong U_\kappa(a)$.*

As an immediate consequence of Lemma 1 we have

LEMMA 2. *Let $A$ have a unit element. $A$ is quasi-Frobeniusean if and only if there is a permutation $(\pi(1), \pi(2), \cdots, \pi(k))$ of $(1, 2, \cdots, k)$ such that for each $\kappa$*

i) *$e_\kappa A$ has a unique simple right subideal $\mathfrak{r}_\kappa$ and $\mathfrak{r}_\kappa \cong \bar{e}_{\pi(\kappa)}\bar{A}$,*

ii) *$Ae_{\pi(\kappa)}$ has a unique simple left subideal $\mathfrak{l}_{\pi(\kappa)}$ and $\mathfrak{l}_{\pi(\kappa)} \cong \bar{A}\bar{e}_\kappa$.*

*Furthermore, $A$ is Frobeniusean if and only if there is a permutation $(\pi(\kappa))$ which satisfies*

iii) $f(\kappa) = f(\pi(\kappa))$

*besides the above* i), ii).

Let us now note an ingenious characterization of Frobeniusean algebras due to R. Brauer and C. Nesbitt.[13] Namely, let $a_1, a_2, \cdots, a_n$ be a basis of $A$ and let

$$a_\rho a_\sigma = \sum_\tau \alpha_{\rho\sigma\tau} a_\tau \qquad (\alpha_{\rho\sigma\tau} \in F) \tag{4}$$

be its multiplication table. Let $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ be an $n$-dimensional vector (with components from $F$) and consider the matrix

$$P = (\sum_\tau \alpha_{\rho\sigma\tau}\lambda_\tau)_{\rho\sigma} \tag{5}$$

(*parastrophic matrix* of $A$ having $\lambda_\tau$ as values of parameters). Consider further the subspace $H$ of $A$ consisting of all elements $x = \sum \xi_\rho a_\rho$ fulfilling

$$\lambda(x) = \sum \lambda_\rho \xi_\rho = 0, \tag{6}$$

$H$ being a hyperplane in $A$ provided that not all of $\lambda_\rho$ are 0. If $\mathfrak{l}$ is the largest left ideal of $A$ contained in $H$, that is, the sum of all left ideals contained in $H$, then $(\mathfrak{l}:F) = n -$ rank of $P$, because $Ax \subseteq H (x = \sum \xi_\rho a_\rho)$ is equivalent to $P(\xi_\rho) = 0$. Similarly, if $\mathfrak{r}$ is the largest right ideal contained in $H$ then $(\mathfrak{r}:F) = n -$ rank of $P (= (\mathfrak{l}:F))$. In particular, $P$ is non-singular if and only if $H$ contains no ideal[14] except the zero ideal. On the other hand, it is known that the existence of a vector $(\lambda_\tau)$ such that $P$ is non-singular implies the existence of a unit element in $A$.[15] Furthermore, if $S(a)$ and $R(a)$ are the left and the right regular representations defined with respect to the basis $(a_1, a_2, \cdots, a_n)$, then the matrix $P$, with any $(\lambda_\tau)$, intertwines $R(a)$ with $S(a)$, that is, $R(a)P = PS(a)$ (for all $a \in A$). And, if $A$ possesses a unit element then conversely every matrix which intertwines $R(a)$ with $S(a)$ can be expressed in the form (5) with a suitable $(\lambda_\tau)$.[16] On combining these facts we find that *an algebra $A$ is Frobeniusean if and only if there exists a hyperplane in $A$ which contains no ideal except the zero ideal*; for the sake of brevity let us say that such a hyperplane is *non-singular*.

## 3. Main theorems (A)

Let $A$ be an algebra over a field $F$. If $S$ is a set of elements in $A$ we denote, as before, the set of right [left] annihilators of $S$ in $A$ by $r(S)$ $[l(S)]$.

---

[13] Brauer-Nesbitt (3), Nesbitt (13).

[14] By an ideal we mean either a left or a right ideal, not necessarily two-sided.

[15] Frobenius (6). Cf. Nakayama-Nesbitt (11), footnote 7.

[16] For this fundamental theorem of parastrophic matrices see Brauer-Nesbitt (3), Nesbitt (13), Nakayama-Nesbitt (11). Cf. also *Appendix* below.

THEOREM 1. *If $A$ is Frobeniusean then*

$\alpha)$ $\quad \mathfrak{l}(r(\mathfrak{l})) = \mathfrak{l}, \quad r(\mathfrak{l}(\mathfrak{r})) = \mathfrak{r},$

$\beta)$ $\quad (\mathfrak{l}:F) + (r(\mathfrak{l}):F) = (A:F), \quad (\mathfrak{r}:F) + (\mathfrak{l}(\mathfrak{r}):F) = (A:F)$

*for every left ideal $\mathfrak{l}$ and right ideal $\mathfrak{r}$, and conversely.*[17,18]

THEOREM 2. *If $A$ is quasi-Frobeniusean then $\alpha)$ (but not necessarily $\beta)$) holds for every $\mathfrak{l}$ and $\mathfrak{r}$, and conversely.*

To prove these theorems we start with considering two vector spaces $\mathfrak{m}$ and $\mathfrak{n}$ of the same dimensionality, say $m$, over $F$. Let $(u_1, u_2, \cdots, u_m)$ and $(v_1, v_2, \cdots, v_m)$ be any bases of $\mathfrak{m}$ and $\mathfrak{n}$ respectively. Take a non-singular matrix $P = (\pi_{\rho\sigma})$ of order $m$ (with elements from $F$) and consider the corresponding bilinear form $\sum \pi_{\rho\sigma}\eta_\rho\xi_\sigma = (\eta)P(\xi)$. Now, if $\mathfrak{s}$ is a subspace of $\mathfrak{m}$ we denote by $p(\mathfrak{s}) = p(\mathfrak{s}; u, v, P)$ the subspace of $\mathfrak{n}$ consisting of all $y = \sum \eta_\rho v_\rho$ such that

$$P(y, x) = (\eta)P(\xi) = 0 \tag{7}$$

for all $x = \sum \xi_\rho u_\rho$ in $\mathfrak{s}$. Similarly, if $\mathfrak{t}$ is a subspace of $\mathfrak{n}$ we denote by $q(\mathfrak{t}) = q(\mathfrak{t}; u, v, P)$ the subspace of $\mathfrak{m}$ consisting of all $x$ such that (7) holds for all $y$ in $\mathfrak{t}$. Then evidently

LEMMA 3. *$q(p(\mathfrak{s})) = \mathfrak{s}$, $p(q(\mathfrak{t})) = \mathfrak{t}$, $\mathfrak{s} \supseteq \mathfrak{s}_1 \rightleftarrows p(\mathfrak{s}) \subseteq p(\mathfrak{s}_1)$, $(\mathfrak{s}:F) + (p(\mathfrak{s}):F) = m$, and thus $p$ and $q$ give a (1-1) anti-isomorphism between the subspace lattices of $\mathfrak{m}$ and $\mathfrak{n}$.*

(If $(\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_m) = (u_1, u_2, \cdots, u_m)U$ is a second basis of $\mathfrak{m}$ such that $\bar{u}_{t+1}, \cdots, \bar{u}_m$ $(t = m - (\mathfrak{s}:F))$ form a basis of $\mathfrak{s}$ and if $(\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_m) = (v_1, v_2, \cdots, v_m)(U^{-1}P^{-1})'$, then $(\bar{v}_1, \cdots, \bar{v}_t)$ is a basis of $p(\mathfrak{s})$; observe that in terms of the coördinates $(\bar{\xi})$, $(\bar{\eta})$ with respect to the new bases $(\bar{u})$, $(\bar{v})$ the relation (7) reads simply $(\bar{\eta})(\bar{\xi}) = 0$.)

Let now $A$ be a *Frobeniusean* algebra over $F$ and let again (4) be the multiplication table of a basis $a_1, a_2, \cdots, a_n$ of $A$. We apply the above observation to $\mathfrak{m} = \mathfrak{n} = A$ and a non-singular matrix $P$ of the form (5) (which exists by our assumption). Indeed, the corresponding bilinear form $P(y, x)$ $(x, y \in A)$ is simply $\lambda(yx)$ (cf. (6)) as can be verified easily. Hence $p(\mathfrak{s}) = p(\mathfrak{s}; a_\rho, a_\rho, P)$ may be interpreted also in the following manner: $p(\mathfrak{s})$ consists of all $y$ in $A$ such that $y\mathfrak{s} \subseteq H$, where $H$ is the (non-singular) hyperplane corresponding to $P$ defined by (6). Similarly $q(\mathfrak{s}) = q(\mathfrak{s}; a_\rho, a_\rho, P)$ consists of all $y$ satisfying $\mathfrak{s}y \subseteq H$. To indicate this fact let us denote our $p$ and $q$ by $p_H$ and $q_H$.

LEMMA 4. *Let $\mathfrak{l}$ be a left ideal of $A$. Then $q_H(\mathfrak{l})$ is a right ideal and consists of all right annihilators of $\mathfrak{l}$, that is $q_H(\mathfrak{l}) = r(\mathfrak{l})$. Similarly $p_H(\mathfrak{r}) = \mathfrak{l}(\mathfrak{r})$ for a right ideal $\mathfrak{r}$ of $A$.*[19]

PROOF. If $\mathfrak{l}y = 0$ then obviously $y \in q_H(\mathfrak{l})$. If conversely $y \in q_H(\mathfrak{l})$ then

---

[17] Here, as well as in the below, we naturally exclude the extreme case $A = 0$.

[18] For the relation $\alpha)$ cf. Hall (7).

[19] As for another bearing of $p_H$, $q_H$, see 9 below.

$ly \subseteq H$. But the zero ideal is the only ideal contained in $H$. Hence $ly = 0$, $y \in r(l)$. $p_H(\mathfrak{r}) = l(\mathfrak{r})$ can be seen in the same way.

On combining these two lemmas we find the validity of *the first part of Theorem* 1. As to the corresponding part of *Theorem* 2 we want to reduce it to the Frobeniusean case.[20]

To do so let first $A$ be any algebra with a unit element (not necessarily quasi-Frobeniusean). Let $N$, $e_{\kappa,i}$, $e_\kappa(= e_{\kappa,1})$, $c_{\kappa,ij}$, $E_\kappa$, $E$, $f(\kappa)$, etc. have the same significance as before. We consider the subalgebra

$$A^0 = \sum_{\kappa,\lambda} e_\kappa A e_\lambda$$

of $A$. $A^0$ has a unit element $E^0 = \sum_\kappa e_\kappa$, and $N^0 = \sum_{\kappa,\lambda} e_\kappa N e_\lambda = A^0 \cap N$ is the radical of $A^0$. Further, let $g$ be an (arbitrary but fixed) integer not less than any of $f(\kappa)$: $g \geqq f(\kappa)$, and consider the (complete) $g$-rowed matric algebra

$$A^* = (A^0)_g = \sum_{i,j=1}^{g} A^0 C^*_{ij}$$

over $A^0$, $C^*_{ij}$ being a system of matric units commutative with all elements of $A^0$ and linearly independent over $A^0$. The radical of $A^*$ is evidently $N^* = \sum_{i,j} N^0 C^*_{ij}$. Put

$$c^*_{\kappa,ij} = e_\kappa C^*_{ij}, \qquad e^*_{\kappa,i} = c^*_{\kappa,ii}, \qquad E^*_\kappa = \sum_i e^*_{\kappa,i}, \qquad E^* = \sum_\kappa E^*_\kappa.$$

Then $e^*_{\kappa,i} (\kappa = 1, 2, \cdots, k;\ i = 1, 2, \cdots, g)$ form a system of mutually orthogonal idempotent elements and their sum $E^*$ is a unit element of $A^*$. $e^*_{\kappa,i}$ are primitive since the algebras $e^*_{\kappa,i} A^* e^*_{\kappa,i} (\cong e_\kappa A^0 e_\kappa = e_\kappa A e_\kappa)$ are completely primary. Moreover, two left [right] ideals $A^* e^*_{\kappa,i}$ and $A^* e^*_{\lambda,j}$ [$e^*_{\kappa,i} A^*$ and $e^*_{\lambda,j} A^*$] are isomorphic if and only if $\kappa = \lambda$, because $e^*_{\kappa,i} A^* e^*_{\lambda,j} \not\subseteq N^*$ if and only if $\kappa = \lambda$. We denote $e^*_{\kappa,1}$ by $e^*_\kappa$.

Now, if $a$ is an element of our original algebra $A$, we put

$$a(i,j) = \sum_{f(\kappa) \geqq i, f(\lambda) \geqq j} c_{\kappa,1i} a c_{\lambda,j1} \qquad (\in A^0)$$

and we associate with $a$ the element

$$a' = \sum_{i,j} a(i,j) C^*_{ij} \text{ of } A^*;$$

in particular $c_{\kappa,ij}$, $e_{\kappa,i}$ are associated with $c^*_{\kappa,ij}$, $e^*_{\kappa,i} (i, j \leqq f(\kappa))$. Then we obtain, as can be verified easily, an isomorphism between $A$ and a subalgebra

$$A' = \sum_{\kappa,\lambda} \sum_{i=1}^{f(\kappa)} \sum_{j=1}^{f(\lambda)} e^*_{\kappa,i} A^* e^*_{\lambda,j}$$

of $A^*$. (Observe that $a'b' = \sum_{i,j} \sum_h a(i,h) b(h,j) C^*_{ij}$ and

$$\begin{aligned}
\sum_h a(i,h) b(h,j) &= \sum_h \Big(\sum_{f(\kappa) \geqq i, f(\lambda) \geqq h} c_{\kappa,1i} a c_{\lambda,h1}\Big)\Big(\sum_{f(\kappa) \geqq h, f(\lambda) \geqq j} c_{\kappa,1h} b c_{\lambda,j1}\Big) \\
&= \sum_h \sum_{f(\kappa) \geqq i, f(\mu) \geqq h, f(\lambda) \geqq j} c_{\kappa,1i} a c_{\mu,h\lambda} b c_{\lambda,j1} \\
&= \sum_{f(\kappa) \geqq i, f(\lambda) \geqq j} c_{\kappa,1i} a \sum_\mu \sum_{h=1}^{f(\mu)} e_{\mu,h} b c_{\lambda,j1} \\
&= \sum_{f(\kappa) \geqq i, f(\lambda) \geqq j} c_{\kappa,1i} a E b c_{\lambda,j1} = \sum_{f(\kappa) \geqq i, f(\lambda) \geqq j} c_{\kappa,1i} a b c_{\lambda,j1} = ab(i,j).)
\end{aligned}$$

[20] A second proof, which is more straightforward than the present one, will be given in Part II.

$E' = \sum_\kappa \sum_{i=1}^{f(\kappa)} e^*_{\kappa,i}$ is a unit element of $A'$ and $A' = E'A^*E'$. The radical $N'$ of $A'$ is $\sum_{\kappa,\lambda} \sum_{i=1}^{f(\kappa)} \sum_{j=1}^{f(\lambda)} e^*_{\kappa,i} N^* e^*_{\lambda,j} = E'N^*E' = A' \cap N^*$. (Observe that $N^* = \sum_{i,j} N^0 C^*_{ij}$.)

If $\mathfrak{z}^*$ is a two-sided ideal of $A^*$ then $\mathfrak{z}' = A' \cap \mathfrak{z}^* = E'\mathfrak{z}^*E'$ is a two-sided ideal of $A'$ and $A^*\mathfrak{z}'A^* = \mathfrak{z}^*$, while if $\mathfrak{z}'$ is a two-sided ideal of $A'$ then $\mathfrak{z}^* = A^*\mathfrak{z}'A^*$ is a two-sided ideal of $A^*$ and $A' \cap \mathfrak{z}^* = \mathfrak{z}'$, as can easily be seen. Hence $\mathfrak{z}^* \rightleftarrows \mathfrak{z}' = A' \cap \mathfrak{z}^*$ gives a 1-1 correspondence between two-sided ideals of $A^*$ and $A'$, and this correspondence is in accord with annihilation, that is,

$$A' \cap r^*(\mathfrak{z}^*) = r'(\mathfrak{z}'), \qquad A' \cap l^*(\mathfrak{z}^*) = l'(\mathfrak{z}') \quad (\mathfrak{z}' = A' \cap \mathfrak{z}^*);$$

where $r'(S')$, $l'(S')$ $[r^*(S^*)$, $l^*(S^*)]$ with $S' \subseteq A'[S^* \subseteq A^*]$ denote the sets of right and left annihilators of $S'[S^*]$ in $A'[A^*]$ respectively. For, $A' \cap r^*(\mathfrak{z}^*) = A' \cap r^*(A^*\mathfrak{z}'A^*) = A' \cap r^*(\mathfrak{z}'A^*) = r'(\mathfrak{z}'A^*E') = r'(\mathfrak{z}')$. In particular, $r'(N') = A' \cap r^*(N^*)$ amd $l'(N') = A' \cap l^*(N^*)$.

Furthermore, for any $S' \subseteq A'$

$$r'(S') = A' \cap r^*(S') = E'r^*(S')E' = (r^*(S') \cap E'A^*)E'$$

(8) (because $E'r^*(S') \subseteq r^*(S')$)

$$= (r^*(S') \cap r^*(A^*(E^* - E')))E' = r^*(A^*S' \cup A^*(E^* - E'))E'.^{21}$$

Similarly

$$l'(S') = E'l^*(S'A^* \cup (E^* - E')A^*). \tag{9}$$

We now assume that $A$ is *quasi-Frobeniusean* (whence $A'$ is so, too). Let $\pi(\kappa)$ have the same significance as in 2, Definition. For each $\kappa$ $r'(N')e^*_{\pi(\kappa)}$ is a simple left ideal of $A'$ and is isomorphic to $A'e^*_\kappa/N'e^*_\kappa$.[22] Hence $e^*_\kappa r'(N')e^*_{\pi(\kappa)}$ is a simple left ideal of $e^*_\kappa A'e^*_\kappa$. Since $r^*(N^*)e^*_{\pi(\kappa)} = A^*r'(N')e^*_{\pi(\kappa)} = \sum_{i=1}^{g} c^*_{\kappa,i} e^*_\kappa r'(N')e^*_{\pi(\kappa)}$, it follows easily that $r^*(N^*)e^*_{\pi(\kappa)}$ is a simple left ideal of $A^*$ and is isomorphic to $A^*e^*_\kappa/N^*e^*_\kappa$. Similarly $e^*_\kappa l^*(N^*)$ is, for each $\kappa$, a simple right ideal of $A^*$ isomorphic to $e^*_{\pi(\kappa)}A^*/e^*_{\pi(\kappa)}N^*$. Therefore $A^*$ is quasi-Frobeniusean and is even Frobeniusean since the corresponding numbers $f^*(\kappa)$ are all equal to $g$. Hence we can apply to $A^*$ the first part of Theorem 1. Thus if $\mathfrak{l}'$ is a left ideal in $A'$

$$\begin{aligned}
l'(r'(\mathfrak{l}')) &= E'l^*(r'(\mathfrak{l}')A^* \cup (E^* - E')A^*) && \text{(by (9))}\\
&= E'l^*(r^*(A^*\mathfrak{l}' \cup A^*(E^* - E'))E'A^* \cup (E^* - E')A^*) && \text{(by 8))}\\
&= E'l^*(r^*(A^*\mathfrak{l}' \cup A^*(E^* - E')) \cup (E^* - E')A^*) && \text{(because } A^*E'A^* = A^*\text{)}\\
&= E'(l^*(r^*(A^*\mathfrak{l}' \cup A^*(E^* - E'))) \cap l^*((E^* - E')A^*))\\
&= E'((A^*\mathfrak{l}' \cup A^*(E^* - E')) \cap A^*E') && \text{(Theorem 1)}\\
&= E'A^*\mathfrak{l}' = A'\mathfrak{l}' = \mathfrak{l}'.
\end{aligned}$$

[21] $\cup$ means a module sum. ($r(X \underline{\cup} Y) = r(X) \cap r(Y)$ for any moduli $X$, $Y$ in $A$.)

Similarly $r'(l'(\mathfrak{r}')) = \mathfrak{r}'$ for a right ideal $\mathfrak{r}'$ of $A'$. Since $A \cong A'$ this proves the first half of Theorem 2.

## 4. Main theorems (B)

The second parts of Theorems 1, 2 are contained in the following stronger assertions:

THEOREM 3. *Let $A$ be an algebra over a field $F$ and let $N$ be its radical. Let $\alpha$) hold for every nilpotent simple left ideal*[23] $\mathfrak{l}$ *and every nilpotent simple right ideal* $\mathfrak{r}$ *as well as for* $\mathfrak{l} = \mathfrak{r} = N$ *and* $\mathfrak{l} = \mathfrak{r} = 0$. *Then $A$ is quasi-Frobeniusean. If moreover $\beta$) holds for every nilpotent simple left ideal* $\mathfrak{l}$ *and every nilpotent simple right ideal* $\mathfrak{r}$, *then $A$ is Frobeniusean.*

PROOF. Let $A$ satisfy the condition of the theorem, that is, let $\alpha$) hold for nilpotent simple ideals as well as for $N$ and 0. Evidently $N \neq A$, for otherwise $l(r(0)) = l(A) = l(N) \geqq N^{\rho-1} \neq 0$ where $\rho$ is the smallest exponent such that $N^\rho = 0$. Furthermore $r(A) = l(A) = 0$, because $A = l(0) = r(0)$. Let $e_{\kappa,i}$, $e_\kappa (= e_{\kappa,1})$, $E_\kappa$, $E$, etc. have the same meaning as before. We proceed stepwise:

i) $\alpha$) and $\beta$) hold for every non-nilpotent (whence idempotent) simple left [right] ideal. For, if $\mathfrak{l}$ is such, $\mathfrak{l}$ is, as is well known, generated by an idempotent element $e$, $\mathfrak{l} = Ae$. $r(\mathfrak{l}) = r(e)$ consists of all elements of the form $a - ea (a \in A)$. Let $c \in l(r(\mathfrak{l}))$. Then $(c - ce)a = c(a - ea) = 0$ for all $a \in A$. Since $l(A) = 0$ it follows $c - ce = 0$, that is, $c = ce \in Ae = \mathfrak{l}$. Hence $l(r(\mathfrak{l})) = \mathfrak{l}$.

Next we want to show that (not only the left ideal $\mathfrak{l} = Ae$ but also) the right ideal $eA$ is simple. For that purpose, suppose that $eA$ is not simple and take a simple right subideal $\mathfrak{r}$ of $eA$. Since $e$ is primitive and $eN$ is the only maximal right subideal of $eA$,[24] $\mathfrak{r}$ is contained in $eN$ and is nilpotent. Hence $r(l(\mathfrak{r})) = \mathfrak{r}$ by our assumption. On the other hand $l(\mathfrak{r}) \supseteq l(eA) = l(e)$ and $A = Ae + l(e)$.[25] But $l(\mathfrak{r}) \neq A$, for $r(l(\mathfrak{r})) = \mathfrak{r} \neq 0$. Since $Ae = \mathfrak{l}$ is simple necessarily $l(\mathfrak{r}) = l(e)$ and $\mathfrak{r} = r(l(\mathfrak{r})) = r(l(e))$. However $r(l(e)) = eA$ as can be seen in the same way as above. Thus we have been led to a contradiction. Hence $eA$ must be a simple right ideal.

Now that both $Ae$ and $eA$ are simple it is easy to see $(Ae{:}F) = (eA{:}F)$.[26] But $A = eA + r(e) = eA + r(\mathfrak{l})$. Thus $(\mathfrak{l}{:}F) = (Ae{:}F) = (eA{:}F) = (A{:}F) - (r(\mathfrak{l}){:}F)$, that is, $\beta$) holds for $\mathfrak{l}$.

ii) Right ideals $e_{\kappa,i}r(N)$ $(\kappa = 1, 2, \cdots, k;\ i = 1, 2, \cdots, f(\kappa))$ are all simple and $l(e_{\kappa,i}r(N)) = N \cup A(E - e_{\kappa,i})$. To prove this let $e$ be one of $e_{\kappa,i}$. $er(N) \neq 0$ since $e \notin N = l(r(N))$. Take a simple right subideal $\mathfrak{r}$ of $er(N)$. $r(l(\mathfrak{r})) = \mathfrak{r}$

[22] Lemma 2. Cf. a remark at the end of 1.

[23] A simple left [right, two-sided] ideal is either idempotent or nilpotent.

[24] See footnote 11.

[25] Peirce decomposition.

[26] Indeed (irreducible) representations defined by $Ae$ and $eA$ are equivalent. $AeA$ is a simple two-sided ideal of $A$ which itself is a simple algebra.

either by our assumption or by i). Furthermore $l(\mathfrak{r}) \supseteq l(er(N))$ and this latter contains in turn $N \cup A(E-e)$. But $N \cup A(E-e)$ is a maximal left ideal. Hence necessarily $l(\mathfrak{r}) = N \cup A(E-e)$ (because $l(\mathfrak{r}) \neq A$) and $\mathfrak{r}(= r(l(\mathfrak{r}))) = r(N \cup A(E-e))$. $er(N)$ lies between the two members of this last equality, whence $er(N) = \mathfrak{r}$. Thus $er(N)$ is simple and $l(er(N)) = N \cup A(E-e)$.

iii) $r(N) = l(N)$. For, since $r(A) = 0$ every simple left ideal must be isomorphic to one of $\bar{A}\bar{e}_\kappa (\kappa = 1, 2, \cdots, k)$. But $E\bar{A}\bar{e}_\kappa = \bar{A}\bar{e}_\kappa$. Hence $r(N) = Er(N) = \sum_{\kappa,i} e_{\kappa,i} r(N)$, because $r(N)$ is the sum of all simple left ideals. The *right* ideals $e_{\kappa,i} r(N)$ are all simple, as was shown in ii), and therefore $r(N) \subseteq l(N)$. Similarly $l(N) \subseteq r(N)$.

iv) $E$ is a unit element of $A$. To see this, suppose $\mathfrak{l}_0 \neq 0$ in the decomposition (1) of $A$ (Section 1), and take a simple left subideal $\mathfrak{l}$ of $\mathfrak{l}_0$. Then $\mathfrak{l}A = 0$, for $\mathfrak{l}E \subseteq \mathfrak{l}_0 E = 0$, $\mathfrak{l}\mathfrak{r}_0 \subseteq r(N)N = l(N)N = 0$ and $A = EA + \mathfrak{r}_0$ (See (1)). Hence $\mathfrak{l} \subseteq l(A) = 0$, contrary to our construction. Thus necessarily $\mathfrak{l}_0 = 0$. Similarly $\mathfrak{r}_0$(of (1)) $= 0$, and this proves the assertion.

v) Denote $r(N) = l(N)$ by $M$. Then two-sided ideals[27] $E_\kappa M$, $ME_\kappa$ are simple. For the proof, take any non-zero element $m = \sum_{i=1}^{f(\kappa)} m_i (m_i \in e_{\kappa,i} M)$ in $E_\kappa M = \sum_i e_{\kappa,i} M$. Suppose $m_1 \neq 0$ for instance. Then $m_1 A = e_\kappa M$ since $e_\kappa M$ is simple. Hence $e_{\kappa,i} M = c_{\kappa,i1} m_1 A = c_{\kappa,i1}(e_\kappa m)A \subseteq AmA$ and $AmA = E_\kappa M$. This shows that $E_\kappa M$ is simple. That $ME_\kappa$ is simple can be proved in the same way.

Now, from $M = \sum_\kappa E_\kappa M = \sum_\kappa ME_\kappa$ it follows that there exists a (unique) permutation $(\pi(1), \pi(2), \cdots, \pi(k))$ of $(1, 2, \cdots, k)$ such that $E_\kappa M = E_\kappa ME_{\pi(\kappa)} = ME_{\pi(\kappa)}$.

vi) $e_\kappa M$ is, for each $\kappa$, a unique simple right subideal of $e_\kappa A$,[28] and is isomorphic to $\bar{e}_{\pi(\kappa)}\bar{A}$ since $e_\kappa ME_{\pi(\kappa)} = e_\kappa M$. Similarly $Me_{\pi(\kappa)}$ is a unique simple left subideal of $Ae_{\pi(\kappa)}$ and $\cong \bar{A}\bar{e}_\kappa$.

Thus $A$ is *quasi-Frobeniusean* according to Lemma 2.

vii) $\bar{e}_\kappa \bar{A} \bar{e}_\kappa \cong \bar{e}_{\pi(\kappa)} \bar{A} \bar{e}_{\pi(\kappa)}$. For, since $e_\kappa M$ is a simple right module of $\bar{A} = A/N$ isomorphic to $\bar{e}_{\pi(\kappa)}\bar{A}$, $\mathfrak{m} = e_\kappa M e_{\pi(\kappa)}$ is a simple right module of the division algebra $\bar{e}_{\pi(\kappa)} \bar{A} \bar{e}_{\pi(\kappa)}$. If $m$ is a non-zero element in $\mathfrak{m}$ then $\mathfrak{m} = m\bar{e}_{\pi(\kappa)}\bar{A}\bar{e}_{\pi(\kappa)}$. Similarly $\mathfrak{m}$ is a simple left module of $\bar{e}_\kappa \bar{A} \bar{e}_\kappa$ and $\mathfrak{m} = \bar{e}_\kappa \bar{A} \bar{e}_\kappa m$. If we associate $a \in \bar{e}_\kappa \bar{A} \bar{e}_\kappa$ with $a' \in \bar{e}_{\pi(\kappa)} \bar{A} \bar{e}_{\pi(\kappa)}$ such that $am = ma'$, then we obtain an isomorphism between the two division algebras. (Observe that $bam = bma' = mb'a'$.)

We now assume that $\beta$) holds for all nilpotent simple ideals; that $\beta$) holds for all non-nilpotent simple ideals was seen in i).

viii) Then $f(\kappa) = f(\pi(\kappa))$ for every $\kappa$. For, $(e_\kappa M : F) = (A:F) - (l(e_\kappa M):F) = (A:F) - (N \cup A(E-e_\kappa):F)$ by ii), and the left-hand side of this equality is equal to $(\bar{e}_{\pi(\kappa)}\bar{A}:F) = f(\pi(\kappa))(\bar{e}_{\pi(\kappa)}\bar{A}\bar{e}_{\pi(\kappa)}:F)$ while the right-hand side is equal to $(\bar{A}\bar{e}_\kappa:F) = f(\kappa)(\bar{e}_\kappa \bar{A} \bar{e}_\kappa : F)$. Hence $f(\pi(\kappa)) = f(\kappa)$ by vii).

---

[27] See 1.

[28] Cf. a remark at the end of 1.

Our algebra $A$ is thus *Frobeniusean*. And this completes the proof.

REMARK. Some of the facts proved in i), ii), $\cdots$, vii) above are of interest by themselves, and they hold (according to the first half of Theorem 2) for any quasi-Frobeniusean algebra.[29] In particular, the relations $r(N) = l(N)$, $E_\kappa M = ME_{\pi(\kappa)}$, $\bar{e}_\kappa \bar{A} \bar{e}_\kappa \cong \bar{e}_{\pi(\kappa)} \bar{A} \bar{e}_{\pi(\kappa)}$ (where $M = r(N) = l(N)$ and $\pi(\kappa)$ has the same significance as in 2, Definition) and the fact that $E_\kappa M = ME_{\pi(\kappa)}$ are simple two-sided ideals will be used later.

## 5. Supplementaries

THEOREM 4. *Let $A$ be a quasi-Frobeniusean algebra and let $c$ be an element in $A$. Then the composition length of the left ideal $Ac$ is equal to that of the right ideal $cA$. If $c = c_1 + c_2$ and $Ac = Ac_1 + Ac_2$ (direct sum) then $cA = c_1A + c_2A$ too, and conversely $c = c_1 + c_2$, $cA = c_1A + c_2A$ implies $Ac = Ac_1 + Ac_2$. If $A$ is Frobeniusean then $(Ac:F) = (cA:F)$.*

PROOF. $a \to ac (a \in A)$ is an (operator-) homomorphic mapping of $A$ onto $Ac$ (with respect to $A$). Left annihilators of $c$ (that is, of $cA$) and only those are mapped onto 0 by this mapping. Hence $A/l(cA) \cong Ac$. On the other hand, the composition length of the left module $A/l(cA)$ is equal to that of the right ideal $cA$ according to Theorem 2. This proves the first assertion of the theorem.

Let now $c = c_1 + c_2$ and $Ac = Ac_1 + Ac_2$. Obviously $cA \subseteq c_1A \cup c_2A$. But the composition lengths of $cA$, $c_1A$, $c_2A$ are respectively equal to those of $Ac$, $Ac_1$, $Ac_2$, and the first of these latter three is equal to the sum of the second and the third since $Ac = Ac_1 + Ac_2$. Hence the composition length of $cA$ is equal to the sum of those of $c_1A$ and $c_2A$, whence necessarily $cA = c_1A + c_2A$.

The last assertion of the theorem is readily seen from $A/l(cA) \cong Ac$ and $(cA:F) + (l(cA):F) = (A:F)$.

COROLLARY. *Let $A$ be Frobeniusean. If a two-sided ideal $\mathfrak{z}$ is a principal left ideal $\mathfrak{z} = Ac$ then $\mathfrak{z} = cA$ too, and conversely.*

PROOF. From the last statement of Theorem 4.

THEOREM 5. *Let $A$ be a quasi-Frobeniusean algebra. If $\mathfrak{l}$ is a (non-zero) left ideal in $A$ and $\mathfrak{l}_0$ is a maximal left subideal of $\mathfrak{l}$ and if the simple left module $\mathfrak{l}/\mathfrak{l}_0$ (of $A$) is isomorphic to $\bar{A}\bar{e}_\kappa$, then the right module $r(\mathfrak{l}_0)/r(\mathfrak{l})$ is isomorphic to $\bar{e}_{\pi(\kappa)}\bar{A}$; where $\pi(\kappa)$ has the same significance as in 2, Definition. Moreover, the division algebra of automorphisms of $\mathfrak{l}/\mathfrak{l}_0$ is inversely isomorphic to the division algebra of automorphisms of $r(\mathfrak{l}_0)/r(\mathfrak{l})$.*

PROOF. Let $b \in r(\mathfrak{l}_0)$. $a \to ab (a \in \mathfrak{l})$ is a homomorphic mapping of the left ideal $\mathfrak{l}$ onto $\mathfrak{l}b$, and indeed $\mathfrak{l}b \cong \mathfrak{l}/\mathfrak{l} \cap l(b)$. Here $\mathfrak{l} \cap l(b)$ is either $\mathfrak{l}$ or $\mathfrak{l}_0$, for $\mathfrak{l} \cap l(b) \supseteq \mathfrak{l} \cap l(r(\mathfrak{l}_0)) = \mathfrak{l}_0$. Therefore either $\mathfrak{l}b = 0$ or $\mathfrak{l}b \cong \mathfrak{l}/\mathfrak{l}_0$ ($\cong \bar{A}\bar{e}_\kappa$). Hence $\mathfrak{l}r(\mathfrak{l}_0)$ is a completely reducible left ideal and is a sum of simple left ideals isomorphic to $\bar{A}\bar{e}_\kappa$. Thus $\mathfrak{l}r(\mathfrak{l}_0) \subseteq E_\kappa M (M = r(N) = l(N))$. Since $\mathfrak{l}r(\mathfrak{l}_0)$ is a

[29] Their validity for quasi-Frobeniusean algebras can easily be proved also directly.

non-zero two-sided ideal and $E_\kappa M$ is a simple two-sided ideal we have $\mathfrak{r}(\mathfrak{l}_0) = E_\kappa M$. Now, $r(\mathfrak{l}_0)$ is a maximal right subideal of $r(\mathfrak{l})$ (by Theorem 2). Suppose $r(\mathfrak{l}_0)/r(\mathfrak{l}) \cong \bar{e}_\lambda \bar{A}$. Then we find in the same way as above that $\mathfrak{r}(\mathfrak{l}_0) = l(r(\mathfrak{l}))r(\mathfrak{l}_0) = ME_\lambda$. Hence $\lambda = \pi(\kappa)$, which proves the first half of the theorem. The second half is then nothing but the relation $\bar{e}_\kappa \bar{A} \bar{e}_\kappa \cong \bar{e}_{\pi(\kappa)} \bar{A} \bar{e}_{\pi(\kappa)}$ already proved before.

THEOREM 6. *Let $A$ be a quasi-Frobeniusean algebra and $N$ be its radical. Then $r(N^\nu) = l(N^\nu)$ $(\nu = 1, 2, \cdots)$.*

PROOF. $r(N) = l(N)$ has been shown. Hence it is sufficient to prove: *If $r(S) = l(S)$ for a subset $S$ of a (not necessarly quasi-Frobeniusean) algebra $A$, then $r(S^\nu) = l(S^\nu)$ for any $\nu \geqq 1$.* To prove this by induction, let $\nu > 1$ and assume that $r(S^{\nu-1}) = l(S^{\nu-1})$. Evidently $l(S^\nu)S \subseteq l(S^{\nu-1})$. Hence $S^{\nu-1}l(S^\nu)S \subseteq S^{\nu-1}l(S^{\nu-1}) = S^{\nu-1}r(S^{\nu-1}) = 0$, $S^{\nu-1}l(S^\nu) \subseteq l(S) = r(S)$ and $S^\nu l(S^\nu) \subseteq Sr(S) = 0$, that is, $l(S^\nu) \subseteq r(S^\nu)$. Similarly $r(S^\nu) \subseteq l(S^\nu)$, whence $r(S^\nu) = l(S^\nu)$.

THEOREM 7. *Let $A$ be an algebra and let $N$ be its radical. If $\alpha$) holds for $\mathfrak{l} = \mathfrak{r} = N$, $\mathfrak{l} = \mathfrak{r} = 0$ and if both $\alpha$) and $\beta$) hold for all nilpotent simple two-sided ideals $\mathfrak{l} = \mathfrak{r} = \mathfrak{z}$, then $A$ is Frobeniusean.*

PROOF. i) $\alpha$) and $\beta$) hold also for every non-nilpotent (whence idempotent) simple two-sided ideal. To prove this let $\mathfrak{z}$ be such. $\mathfrak{z} \cup N/N$ is a simple two-sided ideal of $\bar{A} = A/N$, whence $\mathfrak{z} \cup N/N = \bar{E}_\kappa \bar{A} = \bar{A}\bar{E}_\kappa$ for a certain $\kappa$. On the other hand $\mathfrak{z} \cap r(N) \neq 0$ (since $\mathfrak{z}$ contains at least one simple left ideal) whence $\mathfrak{z} \cap r(N) = \mathfrak{z}$, $\mathfrak{z} \subseteq r(N)$, that is, $\mathfrak{z}$ is a completely reducible left ideal. Moreover, all simple left subideals of $\mathfrak{z}$ are mutually isomorphic, for otherwise $\mathfrak{z}$ would be a direct sum of two non-zero two-sided ideals (consisting of non-isomorphic left ideals). From $\mathfrak{z} \cup N/N = \bar{E}_\kappa \bar{A}$ it follows that those simple left ideals are isomorphic to $\bar{A}\bar{e}_\kappa$. Hence $\mathfrak{z} = E_\kappa \mathfrak{z}$. Similarly $\mathfrak{z} = \mathfrak{z}E_\kappa$, and $\mathfrak{z} \subseteq E_\kappa A E_\kappa$. Since $E_\kappa N E_\kappa$ is a unique maximal two-sided ideal of (the primary algebra) $E_\kappa A E_\kappa$ and since $\mathfrak{z}$ is not contained in $E_\kappa N E_\kappa (\subseteq N)$, necessarily $\mathfrak{z} = E_\kappa A E_\kappa$. Hence $\mathfrak{z}(= \mathfrak{z}A = E_\kappa A E_\kappa A) = E_\kappa A = A E_\kappa$. From $A = E_\kappa A + r(E_\kappa)$[30] $= \mathfrak{z} + r(\mathfrak{z})$ follows now $(A:F) = (\mathfrak{z}:F) + (r(\mathfrak{z}):F)$. This proves $\beta$) for $\mathfrak{z}$. The relation $\alpha$) for $\mathfrak{z}$ can be seen in the same way as in i) of Theorem 3.

ii) Two-sided ideals[31] $E_\kappa r(N)$ $(\kappa = 1, 2, \cdots, k)$ are all simple and $l(E_\kappa r(N)) = N \cup A(E - E_\kappa) (= N \cup A(E - E_\kappa)A = N \cup (E - E_\kappa)A)$. This can be shown in quite a similar manner as in Theorem 3, ii); we have merely to replace $e_{\kappa,i}$ by $E_\kappa$ and $\mathfrak{r}$ by a simple two-sided subideal of $E_\kappa r(N)$ and to notice that $N \cup A(E - E_\kappa)$ is a maximal two-sided ideal of $A$.

iii) $r(N) = l(N)$ and $E$ is a unit element of $A$. For, $E_\kappa r(N) \cap l(N) \neq 0$ (since $E_\kappa r(N)$ contains at least one simple right ideal) whence $E_\kappa r(N) \cap l(N) = E_\kappa r(N)$, $E_\kappa r(N) \subseteq l(N)$. But $r(N) = Er(N) = \sum_\kappa E_\kappa r(N)$, for $r(A) = 0$ (cf. Theorem 3, iii)). Hence $r(N) \subseteq l(N)$. Similarly $r(N) \supseteq l(N)$. That $E$ is a

[30] Peirce decomposition.

[31] See 1.

unit element can be seen from $r(N) = l(N)$ in the same way as before (Theorem 3, iv)).

iv) Denote $r(N) = l(N)$ again by $M$. Then there is a (unique) permutation $(\pi(1), \pi(2), \cdots, \pi(k))$ of $(1, 2, \cdots, k)$ such that $E_\kappa M = ME_{\pi(\kappa)}$.

v) Right ideals $e_{\kappa,i}M$ are all simple. To see this we observe that $E_\kappa M = \sum_{i=1}^{f(\kappa)} e_{\kappa,i}M$ and that $e_{\kappa,i}M$ $(i = 1, 2, \cdots, f(\kappa))$ are mutually isomorphic. Hence $(E_\kappa M:F) = f(\kappa)(e_\kappa M:F)(e_\kappa = e_{\kappa,1})$. On the other hand $(E_\kappa M:F) = (A:F) - (l(E_\kappa M):F) = (A:F) - (N \cup A(E - E_\kappa):F) = f(\kappa)(\bar{e}_\kappa \bar{A}:F)$. Hence $(e_\kappa M:F) = (\bar{e}_\kappa \bar{A}:F)$. But $e_\kappa M$ is a sum of simple left ideals isomorphic to $\bar{e}_{\pi(\kappa)}\bar{A}$, and therefore $(\bar{e}_{\pi(\kappa)}\bar{A}:F) \leqq (\bar{e}_\kappa \bar{A}:F)$. Since this is the case for every $\kappa$, necessarily holds the equality sign and we find that $e_\kappa M$ is simple.

The rest of the proof can be carried out in almost the same way as before (Theorem 3, vi), vii) and viii)); $l(e_{\kappa,i}M) = N \cup A(E - e_{\kappa,i})$ follows from $l(e_{\kappa,i}M) \supsetneqq A$ and the maximality of $N \cup A(E - e_{\kappa,i})$.

We have further

THEOREM 8. *Let our underlying field $F$ be algebraically closed. Let $\alpha$) hold for all nilpotent simple two-sided ideals $\mathfrak{l} = \mathfrak{r} = \mathfrak{z}$ as well as for $\mathfrak{l} = \mathfrak{r} = N$ and $\mathfrak{l} = \mathfrak{r} = 0$. Then $A$ is quasi-Frobeniusean.*

PROOF. i), ii), iii) and iv) (but not v)) of the above proof of Theorem 7 remain valid in our case. We want to prove further that right ideals $e_{\kappa,i}M$ are all simple. For this purpose, let $\mathfrak{r}$ be a simple right subideal of $e_\kappa M$. Then $\sum_{i=1}^{f(\kappa)} c_{\kappa,i1}\mathfrak{r}$ is (not only a right ideal but also) a two-sided ideal, for $A$ is, because of our assumption about $F$, the sum of $\sum_{i,j=1}^{f(\kappa)} Fc_{\kappa,ij}$ and $N \cup A(E - E_\kappa) = l(E_\kappa M)(\subseteq l(\sum_i c_{\kappa,i1}\mathfrak{r}))$. Therefore $\sum_i c_{\kappa,i1}\mathfrak{r} = E_\kappa M$ since $E_\kappa M$ is simple. Hence $\mathfrak{r} = e_\kappa M$ and $e_\kappa M$ is simple.

Our theorem is now immediate; cf. Theorem 3, vi).

REMARK AND EXAMPLE. Our restriction about $F$ in Theorem 8 is not redundant. To see this, let $F$ be a field which possesses a quadratic over-field $K$ and consider an algebra $A$ over $F$ consisting of all matrices of the form

$$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & c & \alpha \end{pmatrix}; \qquad a, b, c \in K, \alpha \in F.$$

The radical $N$ of $A$ is formed of those matrices in which $\alpha = a = 0$, and $r(N) = l(N) = N$. Putting first $\alpha = 1, a = b = c = 0$ and next $a = 1, \alpha = b = c = 0$ we get two mutually orthogonal idempotent elements $E_1$ and $E_2$. $A$, $N$, $0$, $E_1N = NE_2$, $E_2N = NE_1$, $AE_1A$ and $AE_2A$ are the only two-sided ideals of $A$, and if $\mathfrak{z}$ is any one of these then $l(r(\mathfrak{z})) = r(l(\mathfrak{z})) = \mathfrak{z}$. But $A$ is not quasi-Frobeniusean.

Further, it is perhaps useful to give an example of a quasi-Frobeniusean algebra which is not Frobeniusean. An algebra consisting of all matrices

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \gamma_1 & 0 & 0 & 0 \\ \alpha_{21} & \alpha_{22} & \gamma_2 & 0 & 0 & 0 \\ 0 & 0 & \beta & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta & \delta_1 & \delta_2 \\ 0 & 0 & 0 & 0 & \alpha_{11} & \alpha_{12} \\ 0 & 0 & 0 & 0 & \alpha_{21} & \alpha_{22} \end{pmatrix},$$

where $\alpha$'s, $\beta$, $\gamma$'s and $\delta$'s are all $\epsilon F$, is indeed such.

## 6. Residue class algebras

In this section we want to examine under what condition a residue class algebra of a Frobeniusean algebra would be again Frobeniusean.

Let $A$ be a Frobeniusean algebra over $F$, and let $H$ be a non-singular hyperplane in $A$. Furthermore, let $p_H$ and $q_H$ have the same significance as in 3. We saw in Lemma 4 that if $\mathfrak{l}$ is a left ideal of $A$ then $q_H(\mathfrak{l})$ is a right ideal and coincides with $r(\mathfrak{l})$. But, also $p_H(\mathfrak{l})$ is a right ideal, for $x\mathfrak{l} \subseteq H$ implies $xA\mathfrak{l} \subseteq H$.[32]

If $c$ is a non-zero element in $A$ then $p_H(cF)$ is a hyperplane in $A$ and conversely every hyperplane in $A$ can be expressed in this form with a suitable non-zero element $c$, as is readily seen from Lemma 3.

LEMMA 5. *The hyperplane $H' = p_H(cF)$ contains the right ideal $p_H(Ac)$ and this is really the largest right ideal contained in $H'$. In particular, $H'$ is non-singular if and only if $c$ is not a divisor of zero.*

PROOF. $H' \supseteq p_H(Ac)$ is evident. If $\mathfrak{r}$ is a right ideal contained in $H'$ then $\mathfrak{r}c \subseteq H$ whence $\mathfrak{r}Ac \subseteq H$, that is, $\mathfrak{r} \subseteq p_H(Ac)$. This proves the lemma.

Now we have

THEOREM 9. *Let $A$ be a Frobeniusean algebra and $\mathfrak{z}$ be a two-sided ideal in $A$. Then the residue class algebra $A/\mathfrak{z}$ is Frobeniusean if and only if the two-sided ideal $r(\mathfrak{z})$ is a principal ideal $cA = Ac$.*

PROOF. Assume that $\bar{A} = A/\mathfrak{z}$ is Frobeniusean, and let $\bar{H}$ be a non-singular hyperplane in $\bar{A}$. Those elements in $A$ whose residue classes (mod $\mathfrak{z}$) lie in $\bar{H}$ form a hyperplane $H'$ in $A$. $\mathfrak{z}$ is the largest right ideal (as well as the largest left ideal) contained in $H'$, for otherwise $\bar{H}$ would contain a non-zero ideal (of $\bar{A}$). Therefore, if $H' = p_H(cF)$ then $p_H(Ac) = \mathfrak{z}$ by the above lemma. Thus $q_H(\mathfrak{z})(= r(\mathfrak{z})) = Ac$. Since $r(\mathfrak{z})$ is two-sided, $r(\mathfrak{z}) = cA$ too (Theorem 4, Corollary).

The converse can be seen easily by reversing the order of the above arguments.

---

[32] Cf. 8 and 9 below.

COROLLARY. *Let $A$ be a Frobeniusean algebra and $\mathfrak{z}$ be a two-sided ideal in $A$. If $r(\mathfrak{z})$ is principal $r(\mathfrak{z}) = Ac = cA$ then $l(\mathfrak{z})$ is principal $l(\mathfrak{z}) = Ad = dA$, and conversely.*

PROOF. We can of course replace $r(\mathfrak{z})$ by $l(\mathfrak{z})$ in Theorem 9. Hence the corollary is immediate.

## 7. Algebras with principal ideals

An algebra $A$ is called *uni-serial* (= *einreihig*) if it has a unit element and is a direct sum of two-sided ideals which themselves are primary algebras and if moreover every left ideal $Ae$ as well as every right ideal $eA$ generated by a primitive idempotent element $e$ possesses only one composition series.[33] As was shown by K. Asano[34] a necessary and sufficient condition that an algebra be uni-serial is that every left ideal as well as every right ideal is principal.[35] On the other hand a uni-serial algebra can be characterized also as an algebra whose residue class algebras are all weakly symmetric in the sense of Nakayama-Nesbitt (11).[36] Now, our Theorem 9 indicates the existence of a similar relationship between Frobeniusean algebras and principal two-sided ideals. Indeed we have

THEOREM 10. *If every residue class algebra of an algebra $A$ is Frobeniusean then for every two-sided ideal $\mathfrak{z}$ of $A$ there exists an element $c$ such that $\mathfrak{z} = Ac = cA$, and conversely.*

PROOF. a) The first half is an immediate consequence of Theorem 9 (and Theorem 1).

b) To prove the second half, assume that for every $\mathfrak{z}$ there exists $c$ satisfying $\mathfrak{z} = Ac = cA$. Then there is in particular an element $c_0$ such that $A = Ac_0 = c_0A$. $l(c_0) = 0$ because otherwise $Ac_0 (\cong A/l(c_0)$ with respect to $A)$ would be smaller than $A$. Moreover there is an element $e$ such that $c_0 = ec_0$. $e$ is idempotent, for $c_0 = ec_0 = e^2c_0$, $(e - e^2)c_0 = 0$ whence $e - e^2 \in l(c_0) = 0$. Therefore $A = Ae + l(e)$ (Peirce decomposition). But here $l(e) = 0$ since otherwise $Ac_0 = Aec_0$ would be smaller than $A$. Hence $A = Ae$ and $e$ is a right-hand unit element of $A$. The existence of a left-hand unit element can be seen in the same way, and thus $A$ has a unit element.

Let $\mathfrak{z} = Ac = cA$. From the mapping $a \to ac$ $(a \in A)$ we obtain $\mathfrak{z} = Ac \cong A/l(c) = A/l(cA) = A/l(\mathfrak{z})$ and $(\mathfrak{z}:F) + (l(\mathfrak{z}):F) = (A:F)$. Since this is the case for every two-sided ideal it follows $r(l(\mathfrak{z})) = \mathfrak{z}$; because $l(r(l(\mathfrak{z})) = l(\mathfrak{z})$[37] whence $(r(l(\mathfrak{z})):F) + (l(\mathfrak{z}):F) = (A:F) = (\mathfrak{z}:F) + (l(\mathfrak{z}):F)$. Similarly $(\mathfrak{z}:F) + (r(\mathfrak{z}):F) = (A:F)$, $l(r(\mathfrak{z})) = \mathfrak{z}$ for every $\mathfrak{z}$. Hence $A$ is Frobeniusean

---

[33] Köthe (9).

[34] Asano (2).

[35] By a principal left, say, ideal we mean here a left ideal expressible as $Ac$; observe that we are not assuming the existence of a unit element.

[36] A weakly symmetric algebra is a Frobeniusean algebra such that $\pi(\kappa) = \kappa$ for all $\kappa$.

[37] $l(r(l(S))) = l(S)$ (and $r(l(r(S))) = r(S)$ for any $S$; because evidently $l(r(l(S))) \supseteq l(S)$ while $r(l(S)) \supseteq S$ whence $l(r(l(S))) \subsetneq l(S)$.

by Theorem 7. That every residue class algebra of $A$ is so too follows then from Theorem 9.

Now the following theorem is of some interests for us, since an algebra of the type discussed in Theorem 10 satisfies its assumption[38] as can readily be verified.[39]

THEOREM 11. *Let $A$ be an algebra with a unit element and such that every left ideal $Ae$ as well as every right ideal $eA$ generated by a primitive idempotent element $e$ has only one composition series.*[40,41] *Then every left [right] module of $A$ is a direct sum of directly indecomposable cyclic submoduli each of which is homomorphic to one of $Ae_\kappa[e_\kappa A]$ ($\kappa = 1, 2, \cdots, k$).*

Our theorem is true also for infinite moduli. But since we shall treat that case in Part II let us in the following proof restrict ourselves to finite moduli:

PROOF. Under this restriction our assertion is equivalent to saying that every directly indecomposable left [right] (finite) module of $A$ is cyclic and is homomorphic to one of $Ae_\kappa[e_\kappa A]$.

Let $\mathfrak{m}$ be a directly indecomposable left (finite) module of $A$ and let $\sigma$ be the smallest exponent such that $N^\sigma\mathfrak{m} = 0$. Since with $A$ every $A/N^\nu$ ($\nu = 1, 2, \cdots$) satisfies the condition of the theorem we may, and shall, assume without loss of generality that $N^\sigma = 0$. Let $u_1, u_2, \cdots, u_s$ be a system of generators of $\mathfrak{m}$. Then $\mathfrak{m}$ is the sum of $Ae_{\kappa,i}u_q$ ($\kappa = 1, 2, \cdots, k$; $i = 1, 2, \cdots, f(\kappa)$; $q = 1, 2, \cdots, s$), and there exists by our assumption at least one triple $(\kappa, i, q)$ such that $N^{\sigma-1}e_{\kappa,i}u_q \neq 0$. Let $(\kappa, i, q)$ be such and put $e = e_{\kappa,i}$, $u = u_q$ for the sake of brevity. Then the submodule $Aeu$ of $\mathfrak{m}$ is (not only homomorphic but also) isomorphic to $Ae$, for $N^{\sigma-1}e$ is the only simple left subideal of $Ae$. Thus a representation $M(a)$ of $A$ belonging to $\mathfrak{m}$ can be reduced to the form

$$\begin{pmatrix} * & 0 \\ * & M_0(a) \end{pmatrix}$$

where $M_0(a)$ belongs to the left ideal $Ae$.

Consider next a *right* representation module $\mathfrak{n}_0$ belonging to the representation $M_0(a)$. It has only one maximal submodule, for $Ae$ has only one simple left subideal. Hence $\mathfrak{n}_0$ is, by Lemma 1, homomorphic to one of $e_\kappa A$ ($\kappa = 1, 2, \cdots, k$), say $e_\lambda A$. But the composition length of $e_\lambda A$ is at most $\sigma$ ($N^\sigma = 0$). Therefore necessarily $\mathfrak{n}_0 \cong e_\lambda A$. Then $M_0(a)$ is a direct component of $M(a)$ as was shown in Nakayama-Nesbitt (11), 2, Remark 3. Since $M(a)$ is by assumption directly indecomposable, necessarily $M(a) \cong M_0(a)$, $\mathfrak{m} = Aeu \cong Ae$. This proves our assertion.

---

[38] The converse does not hold.

[39] Cf. the next footnote 40.

[40] $Ae$ has a unique composition series if and only if the left moduli $Ae/Ne$, $Ne/N^2e$, $N^2e/N^3e$, $\cdots$ are all simple; if that is the case $Ae$, $Ne$, $N^2e$, $\cdots$ is really the unique composition series.

[41] We have of course only to assume the property for $e_1, e_2, \cdots, e_k$. (The same is true for the definition of uni-serial algebras.)

## 8. Left and right representation moduli

As a preliminary for the next section the present one aims to study the relationship between left and right representation moduli belonging to mutually equivalent representations of an algebra, which in fact is essentially nothing but the well known relationship between so-called dual vector spaces.[42]

Let $A$ be an algebra over a field $F$, and let $\mathfrak{m}$ and $\mathfrak{n}$ be left and right representation moduli of $A$ belonging to equivalent representations. Let $(u_1, u_2, \cdots, u_m)$ and $(v_1, v_2, \cdots, v_m)$ be any bases of $\mathfrak{m}$ and $\mathfrak{n}$ respectively and let $M(a)$ and $N(a)$ be the corresponding representations of $A$,

$$a(u_1, \cdots, u_m) = (u_1, \cdots, u_m)M(a), \qquad (v_1, \cdots, v_m)a = (v_1, \cdots, v_m)N(a)'.$$

There exists by our assumption a non-singular matrix $P = (\pi_{\rho\sigma})$ transforming $N(a)$ into $M(a)$,

$$P^{-1}N(a)P = M(a). \tag{10}$$

Consider the bilinear form $\sum \pi_{\rho\sigma}\eta_\rho\xi_\sigma = (\eta)P(\xi)$ and let $p(\mathfrak{s}) = p(\mathfrak{s}; u, v, P)$, $q(\mathfrak{t}) = q(\mathfrak{t}; u, v, P)$ have the same significance as in 3. Then not only do $p$ and $q$ give a 1-1 correspondence of vector subspaces of $\mathfrak{m}$ and $\mathfrak{n}$ (Lemma 3), but that correspondence is really in accord with the representation theory. Namely

LEMMA 6. *If $\mathfrak{m}_1$ is a submodule[43] of $\mathfrak{m}$ then $p(\mathfrak{m}_1) = p(\mathfrak{m}_1, u, v, P)$ (with $P$ satisfying* (10)*) is a submodule of $\mathfrak{n}$, and conversely. If $\mathfrak{m}_2$ is a second submodule of $\mathfrak{m}$ which contains $\mathfrak{m}_1$, the representation of $A$ defined by $\mathfrak{m}_2/\mathfrak{m}_1$ is equivalent to the one defined by $p(\mathfrak{m}_1)/p(\mathfrak{m}_2)$.*

PROOF. Let $(\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_m) = (u_1, u_2, \cdots, u_m)U$ be a second basis of $\mathfrak{m}$ such that $\bar{u}_{t+1}, \cdots, \bar{u}_m$ $(t = m - (\mathfrak{m}_1{:}F))$ form a basis of $\mathfrak{m}_1$, and put $(\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_m) = (v_1, v_2, \cdots, v_m)(U^{-1}P^{-1})'$. Then $(\bar{v}_1, \cdots, \bar{v}_t)$ is a basis of $p(\mathfrak{m}_1)$ (see Lemma 3 in 3). The representation defined by the basis $(\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_m)$ of $\mathfrak{m}$ is $U^{-1}M(a)U$ and it has the form

$$U^{-1}M(a)U = \begin{pmatrix} \tilde{M}(a) & 0 \\ * & M_0(a) \end{pmatrix}, \tag{11}$$

where $\tilde{M}(a)$, $M_0(a)$ are representations of $A$ defined by the bases $(\bar{u}_1, \cdots, \bar{u}_t \pmod{\mathfrak{m}_1})$, $(\bar{u}_{t+1}, \cdots, \bar{u}_m)$ of $\mathfrak{m}/\mathfrak{m}_1$, $\mathfrak{m}_1$ respectively. On the other hand the representation defined by the basis $(\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_m)$ of $\mathfrak{n}$ is $U^{-1}P^{-1}N(a)(U^{-1}P^{-1})^{-1}$ and this is nothing but $U^{-1}M(a)U$. The form (11) of $U^{-1}M(a)U$ shows that the subspace $p(\mathfrak{m}_1)$ spanned by $\bar{v}_1, \cdots, \bar{v}_t$ is a submodule.

To prove the second half of the lemma, we choose $(\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_m)$ so that not only do $\bar{u}_{t+1}, \cdots, \bar{u}_m$ form a basis of $\mathfrak{m}_1$ but also $\bar{u}_{r+1}, \cdots, \bar{u}_m$ $(r = m - (\mathfrak{m}_2{:}F))$ form a basis of $\mathfrak{m}_2$. Then the block $\tilde{M}(a)$ in (11) has the form

[42] Weyl (17), Chap. I, §3.

[43] By a submodule we mean an allowable one.

$\tilde{M}(a) = \begin{pmatrix} M_2(a) & 0 \\ * & M_1(a) \end{pmatrix}$ where $M_2(a)$ and $M_1(a)$ denote the representations defined by the basis $(\bar{u}_1, \cdots, \bar{u}_r \pmod{\mathfrak{m}_2})$, $(\bar{u}_{r+1}, \cdots, \bar{u}_t \pmod{\mathfrak{m}_1})$ of $\mathfrak{m}/\mathfrak{m}_2$, $\mathfrak{m}_2/\mathfrak{m}_1$ respectively. The representation corresponding to the basis $(\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_m) = (v_1, v_2, \cdots, v_m)(U^{-1}P^{-1})'$ of $\mathfrak{n}$ is again $U^{-1}M(a)U$, which now has the form

$$\begin{pmatrix} M_2(a) & 0 & 0 \\ * & M_1(a) & 0 \\ * & * & M_0(a) \end{pmatrix}. \tag{12}$$

Thus we see that the representation defined by the basis $(\bar{v}_{r+1}, \cdots, \bar{v}_t \pmod{p(\mathfrak{m}_2)})$ of $p(\mathfrak{m}_1)/p(\mathfrak{m}_2)$ coincides with $M_1(a)$. This completes the proof.

## 9. Symmetric algebras[44]

Let $A$ be an algebra over a field $F$. Let $a_1, a_2, \cdots, a_n$ be a basis of $A$ with a multiplication table (4) (Section 2). Denote by $S(a)$, $R(a)$ the left and the right regular representations of $A$ defined by the basis $a_1, a_2, \cdots, a_n$.

DEFINITION. *$A$ is called symmetric if it possesses a unit element and if there exists a non-singular symmetric matrix which transforms $R(a)$ into $S(a)$.*[45]

It is convenient to characterize a symmetric algebra again in terms of hyperplanes in it. On retaining the notations of 2, we see easily that the matrix $P = (\sum_\tau \alpha_{\rho\sigma\tau}\lambda_\tau)$ ((5)) is symmetric if and only if the linear form $\lambda(x) = \sum \lambda_\tau \xi_\tau$ ((6)) satisfies $\lambda(xy) = \lambda(yx)$ for all $x, y \in A$. This last condition is equivalent to that the corresponding hyperplane $H$, defined by (6), contains all commutator elements $xy - yx$ in $A$; let us say that $H$ is *symmetric* if such is the case. Hence, on combining this with previous considerations we find that $A$ is symmetric if and only if there exists in $A$ a *non-singular symmetric hyperplane.*

To obtain a refinement of the first half of Theorem 1 for symmetric algebras, let first $A$ be merely *Frobeniusean* and consider a non-singular hyperplane $H$ in $A$. As an immediate consequence of Lemma 6 8 we have: *If $\mathfrak{l}$ is a left ideal then $p_H(\mathfrak{l})$ is a right ideal, and conversely.*[46] *If $\mathfrak{l}_0$ is a left subideal of $\mathfrak{l}$ the representation of $A$ defined by $\mathfrak{l}/\mathfrak{l}_0$ is equivalent to the one defined by $p_H(\mathfrak{l}_0)/p_H(\mathfrak{l})$.*

Let now $A$ be *symmetric* and let correspondingly $H$ be a non-singular symmetric hyperplane in $A$. Then $p_H(\mathfrak{s}) = q_H(\mathfrak{s})$ for any subspace $\mathfrak{s}$ of $A$, since $x\mathfrak{s} \subseteq H$ implies $\mathfrak{s}x \subseteq H$ and conversely. In particular, $p_H(\mathfrak{l}) = q_H(\mathfrak{l}) = r(\mathfrak{l})$ for a left ideal $\mathfrak{l}$ (Lemma 4). Therefore

THEOREM 12. *Let $A$ be a symmetric algebra. Then the* 1-1 *correspondence of left and right ideals in $A$ by annihilation, which was established in (the first part of) Theorem* 1, *has the following property: If $\mathfrak{l}_0$ is a left subideal of a left ideal $\mathfrak{l}$, the*

[44] Brauer-Nesbitt (3), Nesbitt (13), Nesbitt (14). Cf. also Nakayama-Nesbitt (11).

[45] That this definition is independent of the special choice of the basis can readily be seen.

[46] This has been shown directly in 6 too.

*representation of $A$ defined by the left module $\mathfrak{l}/\mathfrak{l}_0$ is equivalent to the one defined by the right module $r(\mathfrak{l}_0)/r(\mathfrak{l})$.*

COROLLARY. *Let $A$ be a symmetric algebra and $c$ be an element in $A$. Then the representation of $A$ defined by the principal left ideal $Ac$ is equivalent to the one defined by the principal right ideal $cA$.*

PROOF. This can be seen in the same way as (the first (or the last) statement of) Theorem 4. Indeed the representation defined by $A/l(cA)$ is equivalent to the one defined by $cA$.

We have further

THEOREM 13. *Let $A$ be a symmetric algebra and let $\mathfrak{z}$ be a two-sided ideal in $A$. Then $r(\mathfrak{z}) = l(\mathfrak{z})$, and the residue class algebra $A/\mathfrak{z}$ is symmetric if and only if this two-sided ideal $r(\mathfrak{z}) = l(\mathfrak{z})$ is a principal ideal generated by an element in the center of $A$.*

PROOF. Let $H$ be a non-singular symmetric hyperplane in $A$. Then $r(\mathfrak{z}) = q_H(\mathfrak{z}) = p_H(\mathfrak{z}) = l(\mathfrak{z})$ and this proves the first assertion. Now, consider a second hyperplane $H' = p_H(cF)$ in $A$ (cf. 6). *$H'$ is symmetric if and only if $c$ is in the center of $A$.*[47] To see this, let $H'$ be symmetric. Then $(xy - yx)c \in H'c \subseteq H$ whence $y(cx - xc) = (xy - yx)c - (x(yc) - (yc)x) \in H$ for all $x, y \in A$. Since $H$ is non-singular $cx - xc = 0$ for all $x \in A$, that is, $c$ lies in the center. The converse is immediate, for if $c$ is in the center then $(xy - yx)c = x(yc) - (yc)x \in H$ for all $x, y$.

Let $\tilde{A} = A/\mathfrak{z}$ be symmetric and let $\tilde{H}$ be a non-singular symmetric hyperplane in $\tilde{A}$. Let further $H'$ be the hyperplane in $A$ formed of those elements whose residue classes (mod $\mathfrak{z}$) lie in $\tilde{H}$. That if $H' = p_H(cF)$ $r(\mathfrak{z}) = cA = Ac$ was shown in the proof of Theorem 9. But our $H'$ is evidently symmetric, whence $c$ lies in the center. This proves a half of the second statement of our theorem. The other half is also evident from these considerations.

EXAMPLE. (Ordinary) group algebras (of finite groups) are symmetric.[48] More generally, semilinear group algebras[49] are symmetric. Namely, let $\mathfrak{G}$ be a finite group and let $K/F$ be a (separable) Galois extension whose Galois group is homomorphic to $\mathfrak{G}$, whence isomorphic to a factor group $\mathfrak{G}/\mathfrak{H}$ of $\mathfrak{G}$ with respect to an invariant subgroup $\mathfrak{H}$. On fixing (the subgroup $\mathfrak{H}$ and) the isomorphism we can consider $\mathfrak{G}/\mathfrak{H}$ itself as the Galois group of $K/F$. Furthermore, we understand by $\alpha^R$ ($\alpha \in K$, $R \in \mathfrak{G}$) the conjugate of $\alpha$ corresponding to the co-set of $R$ (mod $\mathfrak{H}$). We consider the algebra

$$A = u_E K + u_R K + \cdots + u_S K; \qquad \mathfrak{G} = \{E, R, \cdots, S\}$$

over $F$ in which the multiplication is defined by $u_R u_S = u_{RS}$, $\alpha u_R = u_R \alpha^R$ ($\alpha \in K$). Then this algebra $A$—a semilinear group algebra—is symmetric. Proof: Let $(\omega_1, \omega_2, \cdots, \omega_m)$ be a normal basis of $K/F$, that is, a basis of $K/F$

[47] The same fact has been formulated in a different way in Nesbitt (14).
[48] Brauer-Nesbitt (3), (4).
[49] Nakayama-Shoda (12).

consisting of the conjugates of one element. $u_E\omega_1$, $u_E\omega_2$, $\cdots$, $u_E\omega_m$, $u_K\omega_1$, $\cdots$, $u_S\omega_m$ form a basis of $A$. Let $H$ be a hyperplane in $A$ consisting of those elements whose coordinates $\xi_{R,\rho}$ with respect to the above basis satisfy $\xi_{E,1} + \xi_{E,2} + \cdots + \xi_{E,m} = 0$; $E$ being the unit element of $\mathfrak{G}$. That $H$ is non-singular is easy to verify. To see that $H$ is symmetric, consider any two basis elements $a = u_K\omega_\rho$ and $b = u_S\omega_\sigma$. $ab = u_{RS}\omega_\rho^S\omega_\sigma$ and $ba = u_{SK}\omega_\sigma^R\omega_\rho$. If $RS \neq E$ then $ab$, $ba \in H$ whence $ab - ba \in H$. If $RS = E$ then $ab - ba = u_E((\omega_\sigma^R\omega_\rho)^S - \omega_\sigma^R\omega_\rho)$. But the coefficients of a conjugate of an element with respect to a normal basis can be obtained from those of that element by a mere permutation. Thus $ab - ba \in H$ also in this case. Hence $H$ is symmetric. (The parastrophic matrix corresponding to this $H$ is the matrix $(\delta_{RS}tr(\omega_\rho^R\omega_\sigma))$, where $\delta_{RS} = 1$ or 0 according as $RS = E$ or not.)

We can further generalize our $A$ by introducing a factor set; we define the multiplication of $u_R$ and $u_S$ by $u_Ru_S = u_{RS}\gamma_{R,S}$ where $\gamma_{R,S}$ are non-zero elements from $K$ such that $\gamma_{R,ST}\gamma_{S,T} = \gamma_{RS,T}\gamma_{R,S}^T$. An algebra thus obtained is also symmetric; the proof runs in exactly the same way as above if we notice that we can assume, without loss of generality, that $u_Eu_R = u_Ru_E = u_R$ for all $R$ and then $\gamma_{R,R^{-1}}^R = \gamma_{R^{-1},R}$. By this generalization we are including collinear group algebras[50] ($\mathfrak{H} = \mathfrak{G}$). Another extreme case is a crossed product ($\mathfrak{H} = E$). In fact, a semisimple algebra is always symmetric.[51] But our theorems are almost trivial for semisimple algebras and our concern lies in non-semisimple symmetric algebras, in particular, in non-semisimple (ordinary, semilinear or collinear) group algebras (over modular fields).

REMARK. Frobeniusean algebras possessing the property stated in Theorem 12 are not necessarily symmetric. On the other hand those algebras are weakly symmetric in the sense of Nakayama-Nesbitt (11),[52] but the converse does not hold. To see these facts, let $\alpha$ and $\beta$ be two different non-zero elements in the underlying field $F$ and consider the algebra $A$ generated by 4 basis elements

$$a_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$a_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ \beta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad a_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

[50] See for instance Tazawa (16).

[51] For the proof we may, after Brauer and Nesbitt, use the fact that the (reduced) discriminant does not vanish. This proof fails in the case where the algebra becomes non-semisimple by an extension of the underlying field, and such a case was discussed in

$A$ is completely primary and weakly symmetric but not symmetric.[53] $N = a_1F + a_2F + a_3F$ is the radical of $A$, and $N^2 = a_1F$, $N^3 = 0$. Besides $A$, $N$, $N^2$, 0 the ideals $Ac = cA = a_1F + cF$ ($c = a_2\xi + a_3\eta$) are the only ideals of $A$. 1) Let first the characteristic of $F$ be different from 2 and put in particular $\beta = -\alpha$. Then $A$ has the property in Theorem 12, as can be verified easily. This proves the first statement of the remark. 2) Let next $\alpha$ and $\beta$ be such that not only $\alpha \neq \beta$ but also $\alpha \neq -\beta$. Consider then $Ac = cA$ with $c = a_2 + a_3$. By a representation belonging to the right representation module $AcA$ the element $a_2\alpha - a_3\beta$ corresponds to a non-zero matrix, while the same element corresponds to zero matrix in a representation defined by the left representation module $AcA$. Thus $A$ does not possess even the property of the corollary.

Furthermore, this last example shows also that the relation $r(\mathfrak{z}) = l(\mathfrak{z})$ does not hold for a weakly symmetric algebra in general. For, $a_2\alpha - a_3\beta \in l(AcA)$ but $\notin r(AcA)$.

## Appendix: On parastrophic matrices

This appendix aims to re-formulate and to generalize that theorem of parastrophic matrices which played a fundamental rôle in our above study.

Let $A$ be an algebra over a field $F$, and let $\mathfrak{m}$ and $\mathfrak{n}$ be respectively any *left* and *right* representation moduli of $A$. Then we introduce a new vector space $\mathfrak{n}*\mathfrak{m}$ generated by formal expressions $v*u$ ($u \in \mathfrak{m}$, $v \in \mathfrak{n}$) *which satisfy the relation*

$$va*u = v*au \qquad (a \in A)$$

*besides* $\alpha(v*u) = \alpha v*u = v*\alpha u$ ($\alpha \in F$), $(v + v')*u = (v*u) + (v'*u)$, $v*(u + u') = (v*u) + (v*u')$. In other words, if $u_1, u_2, \cdots, u_m$ and $v_1, v_2, \cdots, v_n$ are bases of $\mathfrak{m}$ and $\mathfrak{n}$ respectively and if $M(a) = (\mu_{\psi\sigma}(a))$, $N(a) = (\nu_{\rho\varphi}(a))$ are the representations of $A$ defined by these bases of $\mathfrak{m}$ and $\mathfrak{n}$, then $\mathfrak{n}*\mathfrak{m}$ is a free $F$-module generated by $nm$ symbols $v_\rho*u_\sigma$ with a system of defining relations

$$(13) \qquad \sum_{\varphi=1}^{n} \nu_{\rho\varphi}(a)(v_\varphi*u_\sigma) - \sum_{\psi=1}^{m} \mu_{\psi\sigma}(a)(v_\rho*u_\psi) = 0, \qquad a \in A.$$

Let $t_1, t_2, \cdots, t_h$ be a basis of $\mathfrak{n}*\mathfrak{m}$. Put

$$v_\rho*u_\sigma = \sum_\tau \omega_{\rho\sigma\tau} t_\tau$$

and denote by $T$ the $(h, nm)$-matrix $(\omega_{\rho\sigma\tau})_{\tau,\rho\sigma}$. Thus $(v_1*u_1, v_1*u_2, \cdots, v_n*u_m) = (t_1, t_2, \cdots, t_h)T$. If $\mathfrak{t}_{11}, \mathfrak{t}_{12}, \cdots, \mathfrak{t}_{nm}$ denote the $nm$ columns of $T$,

---

Nakayama-Nesbitt (11), footnote 16. However the description there was not so clear. It is true that we can achieve our aim by means of Theorem 5 there, but we should have referred rather to Theorem 4. Namely, the problem can be easily reduced to the case of a simple algebra and then to the case of a normal simple algebra by that Theorem 4.

[53] See footnote 36 above.

[53] Nakayama-Nesbitt (11), 2.

the only (linear homogeneous) relations existing among them are those which are consequences of

$$\sum_\varphi \nu_{\rho\varphi}(a)\mathfrak{t}_{\varphi\sigma} - \sum_\psi \mu_{\psi\sigma}(a)\mathfrak{t}_{\rho\psi} = 0.$$

Now we have: *Every matrix $P$ intertwining $N(a)$ with $M(a)$ (that is, satisfying $N(a)P = PM(a)$) can be expressed in the form*

$$P = \left(\sum_{\tau=1}^{h} \omega_{\rho\sigma\tau}\lambda_\tau\right)_{\rho\sigma} \tag{14}$$

*with a suitable vector $(\lambda_\rho)$, and conversely every matrix of the form* (14) *intertwines $N(a)$ with $M(a)$.* Proof: 1) That a matrix $P = (\pi_{\rho\sigma})$ intertwines $N(a)$ with $M(a)$ is equivalent to that

$$\sum_{\varphi=1}^{n} \nu_{\rho\varphi}(a)\pi_{\varphi\sigma} - \sum_{\psi=1}^{m} \mu_{\psi\sigma}(a)\pi_{\rho\psi} = 0 \qquad (\text{for all } a \in A).$$

Thus $\pi_{11}, \pi_{12}, \cdots, \pi_{nm}$ satisfy all linear relations existing among the $nm$ columns $\mathfrak{t}_{11}, \mathfrak{t}_{12}, \cdots, \mathfrak{t}_{nm}$ of $T$. Hence the $(h+1, nm)$-matrix obtained from $T$ by adding a row $(\pi_{11}, \pi_{12}, \cdots, \pi_{nm})$ has the same rank $h$ as $T$. There exists therefore a vector $(\lambda_\tau)$ such that $(\lambda_1, \lambda_2, \cdots, \lambda_h)T = (\pi_{11}, \pi_{12}, \cdots, \pi_{nm})$. But this expresses nothing else but (14) (cf. the definition of $T$). 2) The converse is obvious also from the above consideration.

(Let now $H$ be a subspace in $\mathfrak{n}*\mathfrak{m}$ consisting of all elements $\sum \zeta_\tau t_\tau$ such that $\sum \zeta_\tau\lambda_\tau = 0$. Let $r$ be the rank of the matrix $P = \left(\sum_\tau \omega_{\rho\sigma\tau}\lambda_\tau\right)$. Since $v*(u_1, u_2, \cdots, u_m) = (\eta_1, \eta_2, \cdots, \eta_n)\left(\sum_\tau \omega_{\rho\sigma\tau}t_\tau\right)$ if $v = \sum \eta_\rho v_\rho$, we find that there exist exactly $n - r$ linearly independent elements $v$ in $\mathfrak{n}$ satisfying $v*\mathfrak{m} \subseteq H$. Combining this fact with the above consideration we see in particular that $M(a)$ can be reduced to the form $\begin{pmatrix} N(a) & 0 \\ * & * \end{pmatrix}$ if and only if there exists a hyperplane $H$ in $\mathfrak{n}*\mathfrak{m}$ such that there is no non-zero element $v$ in $\mathfrak{n}$ satisfying $v*\mathfrak{m} \subseteq H$.)

In the special case where the left module $\mathfrak{m}$ is a residue class module of a left ideal $\mathfrak{l}$ with respect to a left subideal $\mathfrak{l}_0$: $\mathfrak{m} = \mathfrak{l}/\mathfrak{l}_0$, the vector space $\mathfrak{n}*\mathfrak{m}$ can be mapped homomorphically onto $\mathfrak{n}\mathfrak{l}/\mathfrak{n}\mathfrak{l}_0$ by means of the mapping $v*(l \bmod \mathfrak{l}_0) \to vl \bmod \mathfrak{n}\mathfrak{l}_0$ $(l \in \mathfrak{l})$. If furthermore $\mathfrak{l}$ is generated by an idempotent element $e$: $\mathfrak{l} = Ae$, then this mapping is 1-1 and the vector space $\mathfrak{n}*\mathfrak{m}$ is isomorphic to $\mathfrak{n}\mathfrak{l}/\mathfrak{n}\mathfrak{l}_0$.[54] For, every element of $\mathfrak{n}*\mathfrak{m}$ $(\mathfrak{m} = Ae/\mathfrak{l}_0)$ can be brought into the form $v*(e \bmod \mathfrak{l}_0)$ and if $ve \equiv v'e \bmod \mathfrak{n}\mathfrak{l}_0$ then $v*(e \bmod \mathfrak{l}_0) = v'*(e \bmod \mathfrak{l}_0)$ since $(v - v')*(e \bmod \mathfrak{l}_0) = (ve - v'e)*(e \bmod \mathfrak{l}_0) \in \mathfrak{n}\mathfrak{l}_0*(e \bmod \mathfrak{l}_0) = \mathfrak{n}*(\mathfrak{l}_0 e \bmod \mathfrak{l}_0) = n*0 = 0$. In particular, if $\mathfrak{m} = Ae$ (with an idempotent element $e$) then our multiplication $v*l$ $(l \in Ae)$ is essentially the same thing as the usual $vl$. Thus if $A$ has a unit element and $\mathfrak{m} = A$, $\mathfrak{n} = A$, then the matrix (14) becomes the parastrophic matrix of $A$.

INSTITUTE FOR ADVANCED STUDY

[54] This case was treated also in Nakayama-Nesbitt (11), Theorem 1.

## BIBLIOGRAPHY

(1) E. Artin, *Zur Theorie der hyperkomplexen Zahlen*, Abh. math. Sem. Hamburg 5 (1928).
(2) K. Asano, *Über verallgemeinerte Abelsche Gruppen mit hyperkomplexem Operatorenring und ihre Anwendungen*, forthcoming in Jap. J. Math.
(3) R. Brauer-C. Nesbitt, *On the regular representations of algebras*, Proc. Nat. Acad. Sci. 23 (1937).
(4) R. Brauer-C. Nesbitt, *On the modular representations of groups of finite order*. I., Univ. Toronto Studies, Math. Series 4 (1937).
(5) M. Deuring, *Algebren*, Ergebn. Math. 4 (1935).
(6) G. Frobenius, *Theorie der hyperkomplexen Grössen*, Sitz.-Ber. Berlin (1903).
(7) M. Hall, *A type of algebraic closure*, forthcoming in Ann. Math.
(8) G. Köthe, *Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist*, Math. Zeitschr. 32 (1930).
(9) G. Köthe, *Verallgemeinerte Abelsche Gruppe mit hyperkomplexem Operatorring*, Math. Zeitschr. 39 (1934).
(10) T. Nakayama, *Some studies on regular representations, induced representations and modular representations*, Ann. Math. 39 (1938).
(11) T. Nakayama-C. Nesbitt, *Note on symmetric algebras*, Ann. Math. 39 (1938).
(12) T. Nakayama-K. Shoda, *Über die Darstellung einer endlichen Gruppe durch halbineare Transformationen*, Jap. J. Math. 12 (1936).
(13) C. Nesbitt, *On the regular representations of algebras*, Ann. Math. 39 (1938).
(14) C. Nesbitt, *On primary algebras*, forthcoming.
(15) E. Noether, *Hyperkomplexe Grössen und Darstellungstheorie*, Math. Zeitschr. 30 (1929).
(16) M. Tazawa, *Über die Darstellung der endlichen verallgemeinerten Gruppen*, Sci. Reports Tohoku Imp. Univ. 23 (1934).
(17) H. Weyl, *The theory of groups and quantum mechanics*.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# ADDITION TO MY NOTE "ON UNITARY METRICS IN PROJECTIVE SPACE"[1]

BY HERMANNN WEYL

(Received May 11, 1939)

The note mentioned in the title dealt with the unitary point-plane and point-point distances, $\| x\xi \|$ and $[\![xx']\!]$ in projective space, and proved that under a change of the projective coördinate system the second distance takes on a factor varying between the same fixed limits $K = \Gamma/\gamma$ and $1/K$ as the first distance. I am indebted to Professor Chevalley for the remark that this is an almost immediate consequence of the elementary fact that for two given points $x$, $x'$ the distance $[\![xx']\!]$ is the maximum of the distance $\| x\xi \|$ of $x$ from all planes $\xi$ going through $x'$.

Indeed, let $y$, $\eta$ be the coördinates in the second system. Then

$$[\![yy']\!] = \| y\eta \| \quad \text{(for a certain plane } \eta \text{ going through } y')$$

$$\leqq K \cdot \| x\xi \| \leqq K \cdot [\![xx']\!]. \tag{1}$$

By exchanging the rôles of the two coördinate systems one finds in the same manner

$$[\![xx']\!] \leqq K \cdot [\![yy']\!]. \tag{2}$$

Arguing in the opposite direction and observing that for given $x$ and $\xi$ the point-plane distance $\| x\xi \|$ is the minimum of $[\![xx']\!]$ for all points $x'$ lying in the plane $\xi$, one realizes that $K$ is the *exact* bound in (1) and in (2). Could one replace $K$ in (2) by a smaller constant $K^*$, then one could improve the inequality for the point-plane distance to the same extent:

$$\| y\eta \| = [\![yy']\!] \quad \text{(for a certain point } y' \text{ lying in the plane } \eta)$$

$$\geqq \frac{1}{K^*} \cdot [\![xx']\!] \geqq \frac{1}{K^*} \cdot \| x\xi \| \tag{3}$$

which is impossible.

The maximum and minimum principle for distances on which our argument is based follows readily from the inequality for scalar products

$$\begin{vmatrix} (x, x), & (x, x'), & (x, x'') \\ (x', x), & (x', x'), & (x', x'') \\ (x'', x), & (x'', x'), & (x'', x'') \end{vmatrix} \geqq 0 \tag{4}$$

[1] Annals of Math. 40 (1939), p. 141.

by setting $x'' = \bar{\xi}$ and assuming $(\xi x') = 0$. (4) then becomes

$$\begin{vmatrix} (x, x), & (x, x') \\ (x', x), & (x', x') \end{vmatrix} \cdot (\xi, \xi) - (x', x') \cdot |(\xi x)|^2 \geqq 0 \quad \text{or}$$

$$[xx']^2 \geqq \|\xi x\|^2.$$

The equality sign will hold if

$$\xi_i = A\bar{x}_i + B\bar{x}'_i; \qquad A = (x', x'), \quad B = -(x, x'),$$

or if

$$x'_i = Cx_i + D\bar{\xi}_i; \qquad C = (\xi, \xi), \quad D = -(\xi x)$$

respectively.

Thus the proof (1) breaks down if the two points $y$, $y'$ coincide; for then we shall have $\eta_i = 0$. (3) breaks down if the point $\eta$ coincides with $y$. But both exceptions are readily removed by an appeal to the principle of continuity.

THE INSTITUTE FOR ADVANCED STUDY

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# AN EXTENSION OF A THEOREM OF REMAK

BY CHARLES HOPKINS

(Received October 16, 1938)

Let $G$ denote a group and let $\Omega$ denote a set of (proper) automorphisms of $G$ which contains at least all the inner automorphisms of $G$. By the term admissible subgroup (a.s.) we shall mean any subgroup $H$ of $G$ such that $H^\theta = H$ for all $\theta$ in $\Omega$. Evidently an admissible subgroup is a normal subgroup of $G$. Regarding $G$ we assume only that the minimal condition holds for admissible subgroups. From this assumption it follows that the set of all admissible subgroups different from the identity subgroup $E$ must contain at least one minimal admissible subgroup (m.a.s.). Let $S$ denote the union of all m.a. subgroups.

THEOREM 1. *The union $S$ is the direct product of a finite number of* m.a. *subgroups—i.e. $S = M_1 \times M_2 \times \cdots \times M_n$, where each $M_i$ is a* m.a.s.

PROOF. We know that $G$ contains at least one m.a. subgroup $M_1$ different from $E$. If $M_1 = S$ our theorem is trivially valid. So we assume $M_1 \subset S$.

Let $M_2$ be any fixed m.a.s. not contained in $M_1$ and denote the union $(M_1, M_2)$ by $U_2$. We write $U_1$ for $M_1$ and assume that $U_i$ has been defined for $i = 1, 2, \cdots k-1$. Then we define $U_k$ to be $(U_{k-1}, M_k)$, where $M_k$ is any fixed m.a.s. not contained in $U_{k-1}$.

LEMMA 1. *For $k \neq 1$, $U_k$ is the direct product*

$$M_1 \times M_2 \times \cdots \times M_k .$$

This assertion is clearly true for $k = 2$, since the cross-cut of the two m.a. subgroups $M_1$ and $M_2$ is itself a m.a.s. and a proper subgroup of both $M_1$ and $M_2$. Let us therefore assume that our lemma is valid for $U_i$, $i = 1, 2, \cdots k-1$. By hypothesis, the m.a.s. $M_k$ is not contained in $U_{k-1}$. Hence the cross-cut $[U_{k-1}, M_k]$ is the identity subgroup $E$. So $U_k = (M_1 \times M_2 \times \cdots \times M_{k-1}, M_k) = M_1 \times M_2 \times \cdots \times M_k$, and our lemma is established.

We now construct the ascending chain

$$C_1 : \qquad U_1 \subset U_2 \subset \cdots \subset U_k \subset \cdots .$$

Let $S_1$ denote the sum of the subgroups $U_i$ in $C_1$—i.e. $S_1$ is the set of all elements of $G$ which occur in at least one $U$ with finite subscript.

Let $S_2$ denote the sum of the terms in the chain

$$C_2 : \qquad M_2 \subset M_2 \times M_3 \subset \cdots \subset M_2 \times \cdots \times M_k \subset \cdots .$$

By $S_j$ we shall mean the sum of the terms in the chain $C_j$, where $C_j$ is obtained from $C_{j-1}$ by deleting $M_{j-1}$ from each term in $C_{j-1}$.

Now each $S_j$ is an admissible subgroup, since each term in the chain $C_j$ is the direct product of admissible subgroups. Furthermore, we see that $S_{j-1}$ is

contained properly in $S_j$, since $S_j$ contains $M_j$, while $S_{j-1}$ does not. From the minimal condition for admissible subgroups we know that the descending chain $S_1 \supset S_2 \supset \cdots$ must terminate in an $S$ with finite subscript—in $S_n$, say. But this is possible only if the ascending chain $C_1$ above terminates in a $U$ with finite subscript. Let $U_n$ denote the last term in $C_1$. Then $S_1 = U_n$, and from Lemma 1 we have $S_1 = M_1 \times \cdots \times M_n$. Since $U_n$ must contain every m.a.s. of $G$—else the chain $C_1$ could be continued to $U_{n+1}$, at least—it follows that $S_1$ is the sum of all m.a. subgroups of $G$. This completes the proof of Theorem 1.

In Theorem 1 we have established the existence of at least one direct decomposition of $S$ into the product of m.a. subgroups. The following result gives a partial answer to the "uniqueness-question."

THEOREM 2. *Let* (1) $S = M_1 \times \cdots \times M_n$ *and* (2) $S = M_1' \times \cdots \times M_{n'}'$ *be any two representations of* $S$ *as the direct product of* m.a. *subgroups. Then* $n = n'$ *and the subscripts in the decomposition* (2) *can be so chosen that* $M_i$ *and* $M_i'$ *are centrally-isomorphic.*

This theorem is a special case of a theorem due to Kořínek.[1] It also can be obtained by modifying one of Fitting's proofs.[2]

From this point on we shall be concerned with the structure of a m.a.s. $M$ of $G$, where $M \neq E$. By the term *normal subgroup of* $M$ we shall mean a subgroup of $M$ which is normal with respect to $M$ (but not necessarily with respect to $G$).

A rather obvious result is the following:

LEMMA 2. *If* $N \neq E$ *is a normal subgroup of* $M$, *then* $M$ *is generated by the conjugates* $N^\theta$ *of* $n$, *where* $\theta$ *varies over the elements of* $\Omega$.

For these conjugates generate an a.s. of $G$, which must be equal to $M$, since $M$ is a m.a.s.

Now the minimal condition for admissible subgroups of $G$ gives us relatively little information concerning $M$. To obtain significant results it seems necessary to impose further restrictions on $M$, and this we shall do by assuming the minimal condition for normal subgroups of $M$. By applying Theorem 1 to $M$ and using Lemma 2, we obtain the following result.

---

[1] V. Kořínek, *Sur la decomposition d'un groupe en produit direct des sousgroupes*, Cas. mat. fys., 66 (1937), p. 264. A correction by Kořínek for Lemma 2.2 may be found in Cas. mat. fys., 67 (1938), pp. 209–210.

[2] Fitting, *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Zeitschrift, Vol. 39 (1934), p. 21.

Although Fitting assumes both the ascending and descending chain conditions for admissible subgroups, neither chain condition is necessary for the proof of our Theorem; we need only to assume the *existence* of the decompositions (1) and (2) above. Let $x_i'$ be any element of $M_i'$ and write $x_i' = x_{i1} \cdot x_{i2} \cdots x_{in}$, where $x_{ij}$ is the component of $x_i'$ in (1) above. From the fact that $M_i'$ and $M_j$ contain no proper admissible subgroups other than $E$, it is easy to show that the correspondence $x_i' \to x_{ij}$ is either the "null-homomorphism" or a (proper) isomorphism of $M_i'$ with $M_j$. Hence each of Fitting's operators $\theta_i$ (l.c. p. 22) is either the null-operator or a (proper) isomorphism. The remainder of his proof is applicable to our theorem, since it is only in establishing that at least one $\theta_i$ is an isomorphism that he uses the double chain condition.

THEOREM 3. *If the minimal condition holds for the normal subgroups of the m.a.s. $M$ of $G$, then $M$ is the direct product of a finite number of simple*[3] *groups.*

The analogue of Theorem 2 asserts that in any two direct decompositions

$$\text{(a)}\quad M = R_1 \times \cdots \times R_m$$

and

$$\text{(b)}\quad M = R_1' \times \cdots \times R_{m'}'$$

we must have $m = m'$, while the subscripts in (b) can be so chosen that $R_i$ and $R_i'$ will be centrally-isomorphic.

From Lemma 2 we can assume that (a) is a direct decomposition in which each $R_i$ is a conjugate of $R_1$ under $\Omega$. If $M$ is non-abelian, then each $R_i$ is non-abelian. Since the center of $M$ is the direct product of the centers of the $R_i$, we see that if $M$ is non-abelian, its center is $E$. In this case, then, the fact that $R_i$ and $R_i'$ are centrally-isomorphic implies that they are identical. When $M$ is non-abelian, therefore, we have the following result:

THEOREM 4. *If the minimal condition holds for normal subgroups of a non-abelian* m.a. *subgroup $M$ of $G$, then $M$ is uniquely representable as the direct product of a finite number of simple groups, which constitute a complete set of conjugates under $\Omega$.*

If $M$ is an abelian group $A$, then it is necessarily of order $p^m$ and type $(1, 1, \cdots, 1)$; such a group is uniquely representable as the direct product of simple groups if, and only if, $m = 1$. From Lemma 2 we know that we can find at least one direct decomposition $A = P_1 \times \cdots \times P_m$, where the components $P_i$, of order $p$, are all conjugates of $P_1$ under $\Omega$. Furthermore, the components of *every* decomposition of $A$ into the direct product of simple groups will be conjugate (under $\Omega$) to a fixed component if, and only if, $\Omega$ contains the group of automorphisms of $M$.

In conclusion, we point out that our theorems are for the most part generalizations of results—originally established by Remak[4]—which appear in the literature mainly in connection with chief composition series. A weaker form of Theorem 1 (and of Theorem 3, also) has recently been obtained by Ore.[5]

TULANE UNIVERSITY,
NEW ORLEANS, LOUISIANA.

---

[3] A minimal normal subgroup of $M$ is necessarily simple; for a normal subgroup of any component in the direct-product decomposition would be a normal subgroup of $M$.

[4] R. Remak, *Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen*, Journal für Math., Vol. 162 (1930), pp. 1–16.

[5] O. Ore, *Structures and Group Theory II*, Duke Mathematical Journal, Vol. 4 (1938), pp. 247–269.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# THE REDUCTION OF THE SINGULARITIES OF AN ALGEBRAIC SURFACE

BY OSCAR ZARISKI

(Received February 15, 1939)

## CONTENTS

Introduction ..... 639
I. Classification of valuations in fields of algebraic functions of two variables ..... 643
II. Uniformization of valuations. Fundamental lemma ..... 649
III. Ideals in the quotient ring of a simple point ..... 659
IV. Quotient rings on normal surfaces ..... 666
V. Normal sequences of quotient rings. "Local reduction" theorem ..... 675
VI. Reduction of the singularities ..... 687

## INTRODUCTION

The reduction of the singularities of an algebraic surface has been studied by several authors, in particular by B. Levi [5], Chisini [2], Albanese [1] and R. J. Walker [9].[1] All these proofs, except the one by Walker, are essentially geometric. The proof by Walker, based in part on a paper by Jung [3], is analytic and is entirely rigorous. We give in this paper an *arithmetic* proof of the reduction theorem, based on the theory of valuations and the theory of ideals in algebraic function fields. From the standpoint of rigor, the arithmetic proof leaves nothing to be desired. We should say that the requirement of rigor is to be regarded as trivially satisfied in the present proof. More significant, however, is the clarification of the problem brought about by the use of the methods of modern algebra. The formal apparatus of ideal theory and the concepts of valuation theory enable one to gain full control of the intricate aspects of the problem, and to see clearly through the logical necessity of the various steps of the reduction process. What is gained concretely thereby is that the center of gravity of the proof is shifted from minute details to underlying concepts. As for these, we insist above all on clear-cut definitions, in order that at no time should it be less than perfectly clear what are the objects we are dealing with.

In a paper [$Z_2$], which appeared in the April issue of the American Journal of Mathematics, we used the operation of "integral closure" as a type of birational transformation for surfaces, and, more generally, for varieties. The operation of integral closure leads to the notion of a *normal variety*. Since

[1] For further references and for a critical review of the various proofs, see our Ergebnisse monograph *Algebraic surfaces*, p. 13–23. We may mention here also an unpublished proof by Du Val, based on a careful fusion of procedures outlined by Severi and by Jung.

these concepts play an essential rôle in the proof, we give here the definition of normal varieties and we state briefly some of their most important properties.

Let $\xi_1, \cdots, \xi_n$ be the coördinates of the general point of an algebraic irreducible $r$-dimensional variety $V_r$ in an affine space $S_n$. *We assume throughout that the underlying field of coefficients, denoted by* $\mathsf{K}$, *is algebraically closed and of characteristic zero.* The field $\mathsf{K}(\xi_1, \cdots, \xi_n)$, of degree of transcendency $r$ over $\mathsf{K}$, shall be denoted by $\Sigma$. We consider a simple transcendental extension $\Sigma'$ of $\Sigma$: $\Sigma' = \Sigma(\omega_0)$. By the *homogeneous coördinates* of the general point of $V_r$ in the projective space $P_n$, we mean the elements $\omega_0, \omega_1 = \omega_0\xi_1, \cdots, \omega_n = \omega_0\xi_n$.

Let $\mathfrak{o} = \mathsf{K}[\xi_1, \cdots, \xi_n]$ be the ring of polynomials in the $\xi$'s. Similarly, let $\mathfrak{o}' = \mathsf{K}[\omega_0, \omega_1, \cdots, \omega_n]$. We say that $V_r$ *is normal in the affine space* $S_n$, if $\mathfrak{o}$ is integrally closed in its quotient field $\Sigma$. *The variety* $V_r$ *is said to be normal in the projective space* $P_n$, if $\mathfrak{o}'$ is integrally closed in $\Sigma'$. If $V_r$ is normal in $P_n$, then it is *a fortiori* normal in the affine space $S_n$, *for any choice of the hyperplane at infinity* ($Z_2$, section 18; compare also with Theorem 13, loc. cit.). From now on we shall mean by a normal variety one which is normal in $P_n$.

The importance of normal varieties is due to the following theorem, proved in $Z_2$ (theorem 11′): *the locus of singular points of a normal* $V_r$ *is an algebraic subvariety of dimension* $\leqq r - 2$. In particular, *a normal surface possesses only a finite number of singular points.*[2]

We associate with a given $V_r$ a *class* of normal varieties which are birationally equivalent to $V_r$. Let $\bar{\mathfrak{o}}'$ be the integral closure of $\mathfrak{o}'$ in $\Sigma'$. The transformation $\omega_i \to t\omega_i$, $i = 0, 1, \cdots, n$, $t \subset \mathsf{K}$, defines an automorphism $\tau$ of $\bar{\mathfrak{o}}'$. An element $\zeta$ of $\bar{\mathfrak{o}}'$ is *homogeneous* of *degree* $\rho$, if $\tau\zeta = t^\rho\zeta$, $t$-arbitrary in $\mathsf{K}$. The homogeneous elements in $\bar{\mathfrak{o}}'$, of a given degree $\rho$, have a finite linearly independent base over $\mathsf{K}$. Let $\eta_0, \eta_1, \cdots, \eta_m$ be such a base. It is possible to prove that *if* $\rho$ *is sufficiently high, then the ring* $\mathsf{K}[\eta_0, \eta_1, \cdots, \eta_m]$ *is integrally closed in its quotient field.* This quotient field (a subfield of $\Sigma'$) is again a simple transcendental extension of $\Sigma$, and the quotients $\eta_i/\eta_0$ are elements of $\Sigma$ (see $Z_2$, section 20). Hence we may regard the $\eta$'s as the homogeneous coördinates of the general point of a *normal* $V_r'$, birationally equivalent to $V_r$. We call $V_r'$ a *derived normal variety* for $V_r$, relative to the *character of homogeneity* $\rho$.

Two derived normal varieties relative to the same character of homogeneity are *projectively equivalent.* More generally, the points of two derived normal varieties (for one and the same $V_r$) are in (1,1) correspondence, *without exceptions,* and *the quotient rings of two corresponding points coincide.*[3] From the

[2] The definition and characteristic properties of a simple point, given in $Z_2$ (sections 1–9), will be found re-stated in the course of the consideration developed in III, 11.

[3] If $P$ is a point on a $V_r$ and if the homogeneous coördinates of $P$ are $a_0, a_1, \cdots, a_n$, we define the quotient ring $Q(P)$ of $P$ as the set of all quotients $f(\omega_0, \omega_1, \cdots, \omega_n)/g(\omega_0, \omega_1, \cdots, \omega_n)$, where $f$ and $g$ are forms of like degree and $g(a_0, a_1, \cdots, a_n) \neq 0$ (compare with III, 10). The hypothesis that $f$ and $g$ are forms of like degree implies that the quotient $f/g$ is an element of $\Sigma$.

standpoint of the analysis of singularities any two derived normal varieties of a given $V_r$ are entirely equivalent. This is so, because to us the structure of the quotient ring $Q(P)$ at a point $P$ is the controlling feature of the type of singularity at the point. Thus, for instance, the following property of $Q(P)$ is characteristic for simple points: *if $\mathfrak{p}_0$ denotes the prime zero-dimensional ideal of $Q(P)$, then $P$ is simple if and only if the ring of residual classes $\mathfrak{p}_0/\mathfrak{p}_0^2$ is a K-module of rank $r$* ($Z_2$, theorem 3.2).

The geometric significance of a normal $V_r$ is the following: *if $V_r$ is normal, then the system of its hyperplane sections is complete* ($Z_2$, Theorem 14). The converse is not true. The geometry of the relationship between a given $V_r$ and a derived normal $V_r'$, whose character of homogeneity is $\rho$, is simply this: *the system of hyperplane sections of $V_r'$ is the complete system,* which is the *$\rho$-fold of the system of hyperplane sections of $V_r$.*

The passage from a $V_r$ to a derived normal variety $V_r'$ is one step of our reduction process. Its effect, for surfaces, is the elimination of all the multiple curves of the surface. This elimination, so troublesome in most of the previous proofs, is here achieved in a relatively simple fashion.

We are now in position to state explicitly the exact procedure of reduction. We start with a normal surface $F$. It has a finite number of singularities. We take one of them, say $P$, as the fundamental point of a suitable quadratic transformation. Namely, we consider those quadratic forms in the homogeneous coördinates of the general point of $F$, which vanish at $P$. We take a linearly independent base for these forms over K and we regard the elements of the base as the homogeneous coördinates of the general point of a new surface $F'$, birationally equivalent to $F$. Or, in geometric terms: we refer the sections of $F$ by the hyperquadrics on $P$ to the hyperplane sections of a new surface $F'$.

The surface $F'$ may not be normal. We pass to a derived normal surface of $F'$, say $F_1$. If $F_1$ still has singularities (and necessarily only a finite number), we apply the same procedure to the new normal surface $F_1$, and so we continue. *Our reduction theorem asserts that after a finite number of steps a normal surface is obtained which is free from singularities* (VI, 21).

We wish now to review briefly the salient points of the proof. We shall not follow necessarily the expository order of the paper, but rather we shall attempt to make clear the inner reasons of the various steps. Certain formalities will have to be dispensed with, since we only wish to bring out the conceptual content of the proof.

By the combined transformation from $F$ to $F_1$ (quadratic transformation and integral closure), the point $P$ is resolved into a fundamental curve on which there may be at most a finite number of singular points of $F_1$. Let $P_1$ be one of them. We take $P_1$ as the fundamental point of our quadratic transformation, getting $F_1'$ and a new derived normal surface $F_2$. Continuing in this fashion we get an infinite sequence of points: $P, P_1, P_2, \cdots$, belonging to

the normal surfaces $F$, $F_1$, $F_2$, $\cdots$ respectively. The question on which depends the solutions of the problem is this: *it should be proved that for some sufficiently high integer $m$, the point $P_m$ (and consequently also the points $P_i$, $i > m$) will be simple.* This is essentially our "local reduction" theorem (V, 20). That this theorem is true at all, is an indication of the importance of the "integral closure" transformations. Under quadratic transformation alone infinite sequences of successive singular points can and do occur, as was pointed out by B. Levi [5].

In algebraic geometry[4] one associates intuitively with a sequence of points, such as the one above, a sequence of *successive infinitely near points* on the original surface $F$, i.e. essentially a branch on $F$, of origin $P$. This branch need not be algebraic, nor even analytic.[5] Now the arithmetic analog of a branch is a *zero-dimensional valuation* of the field $\Sigma$ of rational functions on $F$. Accordingly, we consider the quotient rings $Q(P_i)$, we observe that they form a strictly ascending sequence of integrally closed rings, and we prove that *the limit of the rings $Q(P_i)$ (i.e. their union) is the valuation ring of a zero-dimensional valuation* (see V, 19, where we prove in fact a more general lemma). In this fashion we can get any given zero-dimensional valuation $B$. We have only to take, at each step, the fundamental point $P_i$ on $F_i$ at *the center* of $B$, i.e. at the origin of the branch which $B$ defines on $F_i$. Should then our "local reduction" theorem be true, it is at least necessary (but not at all sufficient) that the following be true: *given any zero-dimensional valuation of $\Sigma$, there exists a projective model $F'$ of $\Sigma$ on which the center of the valuation is at a simple point.* This is our fundamental lemma, proved in Part II. On the basis of this lemma, the valuation $B$ defined by the sequence $\{P_i\}$ can equally well be defined (and in infinitely many ways) by a sequence $\{A_i\}$ of *simple points* (belonging to suitable projective models of $\Sigma$), in the sense that the valuation ring of $B$ is also the limit of the quotient ring $Q(A_i)$. Hence every $Q(P_i)$ is a subring of some $Q(A_j)$, and conversely. The proof is completed by showing that *if $i$ is sufficiently high, then $Q(P_i)$ coincides with some $Q(A_j)$.*

The length of the paper is not entirely due to the lengthiness of the proof. It is due in part to the fact that we treat the entire problem *ab initio*. We also wished to avoid, as much as possible, references to scattered sources, especially when we were not certain whether the reference would exactly cover the topic under consideration. Since the elements of valuation theory are not generally known, we also thought it advisable to devote the first part of the paper to a review and classification of the valuations in fields of algebraic functions of two variables.

---

[4] See for instance C. Segre: *Sulla scomposizione dei punti singolari delle superficie algebriche.* Ann. Mat. pura appl. II. s. Vol. 25 (1897).

[5] In the example of an infinite sequence of successive multiple points given by B. Levi, the corresponding branch is in fact transcendental.

## I. Classification of Valuations in Fields of Algebraic Functions of Two Variables

### 1.

Let $\Sigma$ be a field of algebraic functions of two variables, over an algebraically closed field $\mathsf{K}$ of characteristic zero. The elements of $\mathsf{K}$ shall be called *constants*. A *valuation* $B$ of the field $\Sigma$ is an homomorphic mapping $v$ of the multiplicative group $\Sigma$ (the element zero excluded) upon an ordered abelian additive group $\Gamma$, satisfying the following conditions: if $a \neq 0$ is any element in $\Sigma$ and if $v(a)$ is the corresponding element in $\Gamma$, then

(1) $v(a \cdot b) = v(a) + v(b)$;

(2) $v(a + b) \geqq \min.\ (v(a), v(b))$;

(3) $v(c) = 0$, if $c \neq 0$ is an element of $\mathsf{K}$.

The condition (1) says merely that the mapping $a \to v(a)$ is an homomorphism. We shall exclude the *trivial* valuation, in which $\Gamma$ consist of only the element zero. As a consequence, we must also add the following condition: (4) for some $a \neq 0$ in $\Sigma$, $v(a) \neq 0$. The element $v(a)$ of $\Gamma$ is called the *value* of $a$. We formally assign to the zero element of $\Sigma$ the value $+\infty$.

Valuations of $\Sigma$ are classified first of all according to the structure of the *value group* $\Gamma$. If the ordered group $\Gamma$ *is archimedean*, $B$ is said to be *of rank 1*. In the most general case, one considers the *isolated subgroups* of $\Gamma$. A subgroup $\Gamma'$ of $\Gamma$ is isolated if it has the property that together with any positive element $\alpha$ of $\Gamma$ it contains also all the positive elements $\beta < \alpha$. The element 0 is to be regarded by itself as constituting an isolated subgroup of $\Gamma$. Given two isolated subgroups $\Gamma'$ and $\Gamma''$ of $\Gamma$, one is necessarily a subgroup of the other, say $\Gamma' \subset \Gamma''$, and we say that $\Gamma'$ *precedes* $\Gamma''$. In this sense the isolated proper subgroups of $\Gamma$ form an ordered set $M_\Gamma$, having a definite ordinal type. If $M_\Gamma$ is a finite set, of $n$ elements, we say that $\Gamma$ is of *rank* $n$. The valuation $B$ is then also said to be of rank $n$. It is well known that if $r$ is the degree of transcendency of $\Sigma$ over $\mathsf{K}$, then any valuation of $\Sigma$ is of finite rank $\leqq r$ (see K, p. 116). In our case, we can only have valuations of rank $\leqq 2$.

If $\Gamma$ is of rank 1, it is archimedean and is isomorphic to a subgroup of the additive group of all real numbers. If $\Gamma$ is of the type of the group of all rational integers, we say that $\Gamma$—and also the valuation $B$—is *discrete*. More generally, if $\Gamma$ is of rank $n$, we consider the $n$ isolated subgroups $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$ in descending order ($\Gamma \supset \Gamma_1 \supset \Gamma_2 \supset \cdots \supset \Gamma_n$) and the quotient groups $\Gamma_{i-1}/\Gamma_i$ ($i = 1, \cdots, n$, $\Gamma_0 = \Gamma$). Each quotient group $\Gamma_{i-1}/\Gamma_i$ is an ordered archimedean group. If these $n$ quotient groups are all discrete, we say that the group $\Gamma$ (and the valuation $B$) is *discrete*, of rank $n$.

The question of determining the possible types of valuations of $\Sigma$ can be reduced to the same question for purely transcendental fields, i.e. fields of rational functions of two independent variables. To see this, let $B$ be any

valuation of $\Sigma$ and let $x$ and $y$ be two algebraically independent elements of $\Sigma$ whose values in $B$ are non-negative. Let $\omega$ be any element in $\Sigma$ and let

$$F(x, y, \omega) = A_0(x, y)\omega^\nu + \cdots + A_\nu(x, y) = 0 \tag{1}$$

be the algebraic relation between $x$, $y$, $\omega$, where $\nu = [\Sigma : \mathsf{K}(x, y)]$, the relative degree of $\Sigma$ with respect to $\mathsf{K}(x, y)$. Since $v(F) = +\infty$, there must exist at least two terms, say $A_i\omega^{\nu-i}$, $A_j\omega^{\nu-j}$, $i \neq j$, whose values in $B$ are the same. Hence, assuming $i > j$, we have $v(A_i/A_j) = (i - j)v(\omega)$, $0 < i - j \leqq \nu$. It follows that for *any* element $\omega$ in $\Sigma$ the product $\nu!v(\omega)$ is the value of a rational function of $x$, $y$. The value group $\Gamma'$ of the valuation induced by $B$ in the field $\mathsf{K}(x, y)$ has thus the property of containing the $\nu!$-multiple of every element of $\Gamma$. Hence $\Gamma$ and $\Gamma'$ have the same rank, and $\Gamma$ is discrete if and only if $\Gamma'$ is discrete.

## 2.

Another classification of the valuations of $\Sigma$ is based upon the consideration of the so-called *residue field* $\Sigma^*$ of the valuation. We consider the totality of elements of $\Sigma$ whose value in $B$ is non-negative. The set of these elements forms a ring $\mathfrak{B}$, the *valuation ring* of $B$. The elements of $\mathfrak{B}$ whose value is positive form a prime ideal $\mathfrak{P}$ in $\mathfrak{B}$, the *prime ideal of the valuation*. By the residue field $\Sigma^*$ of the valuation $B$ is meant the field of residual classes of $\mathfrak{B}$ modulo $\mathfrak{P}$: $\Sigma^* \cong \mathfrak{B}/\mathfrak{P}$.[6] Since no constant different from zero has value $> 0$, it follows that $\Sigma^*$ contains a subfield $\mathsf{K}^*$ simply isomorphic to $\mathsf{K}$. Now, quite generally, let $r$ be the degree of transcendency of $\Sigma$, whence also of $\mathfrak{B}$, over $\mathsf{K}$. (Note that $\Sigma$ is the quotient field of $\mathfrak{B}$.) Since $\mathfrak{P}$ is not the zero ideal, its dimension $r^*$ is $< r$. $\Sigma^*$ is of degree of transcendency $r^*$ over $\mathsf{K}^*$. We say that $B$ is an *$r^*$-dimensional valuation*. In our present case $r = 2$ and thus we may have valuations of dimension zero or one.

Let us again consider the field $\mathsf{K}(x, y)$, where $x$ and $y$ are algebraically independent elements in $\Sigma$ and $v(x) \geqq 0$, $v(y) \geqq 0$. Let $B_1$ be the valuation of $\mathsf{K}(x, y)$ induced by $B$ and let $\mathfrak{B}_1$, $\mathfrak{P}_1$ be the valuation ring and the prime ideal of the valuation $B_1$ in $\mathsf{K}(x, y)$. Clearly $\mathfrak{B}_1 \subseteq \mathfrak{B}$ and $\mathfrak{P}_1$ consists of all those elements of $\mathfrak{P}$ which are in $\mathfrak{B}_1$. Hence the residue field $\Sigma_1^* = \mathfrak{B}_1/\mathfrak{P}_1$ of the valuation $B_1$ is a subfield of $\Sigma^*$. Let $\omega^*$ be any element of $\Sigma^*$, and let $\omega$ be some element of $\mathfrak{B}$ belonging to the residual class of $\mathfrak{B}/\mathfrak{P}$ determined by $\omega^*$. We write the equation (1) of algebraic dependence between $x$, $y$, $\omega$, and we consider among the polynomials $A_0(x, y), \cdots, A_\nu(x, y)$ one which has the smallest possible value in $B$. Let, say, $A_h$ be such a polynomial. We may assume $h \neq \nu$, because were $v(A_\nu) < v(A_i)$ for $i = 0, 1, \nu - 1$, then, we would have $v(A_\nu(x, y)) < v(A_i(x, y)\omega^{\nu-i})$, $i = 0, 1, \cdots, \nu - 1$, since $v(\omega) \geqq 0$, and this is impossible. The quotients $A_i/A_h$ have non-negative values in $B$, whence they are elements of $\mathfrak{B}_1$. Let $a_0^*, a_1^*, \cdots, a_{h-1}^*, 1, a_{h+1}^*, \cdots, a_\nu^*$ be the corre-

[6] That $\mathfrak{B}/\mathfrak{P}$ is a field follows from the fact that $\mathfrak{P}$ is divisorless.

sponding residual classes mod $\mathfrak{P}_1$. In view of the homorphism between $\mathfrak{B}$ and $\Sigma^*$ we have the relation:

$$a_0^*\omega^{*\nu} + \cdots + a_{h-1}^*\omega^{*\nu-h+1} + \omega^{*\nu-h} + a_{h+1}^*\omega^{*\nu-h-1} + \cdots + a_\nu^* = 0, \quad a_i^* \subset \Sigma_1^*.$$

Since $\nu - h > 0$, $\omega^*$ is algebraic over $\Sigma_1^*$. Thus, we conclude that $\Sigma^*$ *is an algebraic extension of* $\Sigma_1^*$, and that consequently *the dimension of the valuation* $B$ *equals the dimension of the induced valuation* $B_1$ of $\mathsf{K}(x, y)$.

We shall now review the types of valuations existing in $\Sigma$.

### 3. 1-dimensional valuations (prime divisors of $\Sigma$).

We fix an element $X\, f(x, y)/g(x, y)$ in $\mathfrak{B}_1$ which is algebraically independent on $\mathsf{K}$, modulo $\mathfrak{P}$. In other words, we assume that in the homomorphism between $\mathfrak{B}_1$ and $\Sigma_1^*(= \mathfrak{B}_1/\mathfrak{P}_1)$ the element $X$ is not mapped upon an element of $\mathsf{K}^*$ (note that we have assumed $\mathsf{K}$ to be algebraically closed). Either $x$ or $y$ will actually occur in $f(x, y)/g(x, y)$. Let it be, say, $x$. Then $x$ is algebraically dependent on $X$, $y$, and $\mathsf{K}(x, y)$ is an algebraic extension of $\mathsf{K}(X, y)$. Hence also our original field $\Sigma$ is an algebraic extension of $\mathsf{K}(X, y)$. We may therefore replace the field $\mathsf{K}(x, y)$ by the field $\mathsf{K}(X, y)$. We assume that this has already been done, and that therefore $x$ is not congruent to a constant modulo $\mathfrak{P}$.

We consider the ring of polynomials $R = \mathsf{K}[x, y]$ in $x$ and $y$. The elements of this ring which have positive value in $B_1$ form a prime ideal $\mathfrak{p}$, since the entire ring $\mathsf{K}[x, y]$ is contained in the valuation ring $\mathfrak{B}_1$ of $B_1$. The ideal $\mathfrak{p}$ cannot be zero-dimensional, since a congruence of the form $x \equiv c(\mathfrak{p})$, $c \supset \mathsf{K}$, would imply the congruence $x \equiv c(\mathfrak{P}_1)$, in contradiction with our assumption on $x$. Hence $\mathfrak{p}$ is a 1-dimensional ideal, i.e. $\mathfrak{p}$ is a principal ideal $R \cdot f(x, y)$, where $f$ is an irreducible polynomial. If then $h(x, y)$ is a polynomial, then $v(h(x, y))$ is positive if $h \equiv 0(f)$, and is zero if $h \not\equiv 0(f)$. It follows immediately that: (1) the valuation ring $\mathfrak{B}_1$ of $B_1$ consists of all rational functions which, written in lowest terms, are of the form $g(x, y)/h(x, y)$, $h \not\equiv 0(f)$; (2) $\mathfrak{P}_1 = \mathfrak{B}_1 \cdot (f)$; (3) two elements $g/h$, $g_1/h$ in $\mathfrak{B}_1$ have the same value in $B_1$, if and only if $g$ and $g_1$ are exactly divisible by the same proof of $f$. If then we normalize the value group $\Gamma_1$ of $B_1$ by putting $v(f) = 1$, then the value of any element of $\mathsf{K}(x, y)$ is a rational integer. Namely, if $g$ is exactly divisible by $f^m$ and if $h \not\equiv 0(f)$, then $v(g/h) = m$; if $g \not\equiv 0(f)$, and $h$ is exactly divisible by $f^m$, then $v(g/h) = -m$. We conclude, that *any one-dimensional valuation of a field of algebraic functions of two variables is discrete, of rank* 1.

It is well known that the description of a one-dimensional valuation $B$ of the field $\Sigma$ can be given in terms of the ideal theory of any finite integrally closed domain $\mathfrak{o}$ in $\Sigma$, such that (1) $\mathfrak{o}$ is contained in the valuation ring of $B$ and (2) that the *prime ideal* $\mathfrak{p}$ *of* $B$ *in* $\mathfrak{o}$ (i.e. the set of all elements of $\mathfrak{o}$ having positive value in $B$) is 1-dimensional. For instance, we can take for $\mathfrak{o}$ the ring of integral functions of the elements $x$, $y$ considered above. Every primary ideal in $\mathfrak{o}$ belonging to $\mathfrak{p}$ is a primary component of some power of $\mathfrak{p}$. The

primary component of $\mathfrak{p}^m$ is denoted by $\mathfrak{p}^{(m)}$ (symbolic $m^{\text{th}}$ power of $\mathfrak{p}$). Every element $\alpha$ in $\Sigma$ can be put in the form of a quotient $\alpha = a/b$, where $a$ and $b$ are elements of $\mathfrak{o}$, *not both divisible by* $\mathfrak{p}$. The given valuation $B$ is obtained by putting $v(a/b) = +m$, if $a \equiv 0(\mathfrak{p}^{(m)})$, $a \not\equiv 0(\mathfrak{p}^{(m+1)})$, $b \not\equiv 0(\mathfrak{p})$, and $v(a/b) = -m$, if $a \not\equiv 0(\mathfrak{p})$, $b \equiv 0(\mathfrak{p}^{(m)})$, $b \not\equiv 0(\mathfrak{p}^{(m+1)})$ (see K, p. 37 and p. 104–105).

### 4. Zero-dimensional valuations of rank 2

The order preserving homomorphic mapping of $\Gamma$ upon the quotient group $\Delta_1 = \Gamma/\Gamma_1$ ($\Gamma_1$, the isolated subgroup) defines an homomorphic mapping of $\Sigma$ upon the ordered group $\Delta_1$, of rank 1, i.e. a valuation $B_1$ of $\Sigma$, of rank 1. Let $\mathfrak{B}_1$ be the valuation ring of $B_1$, $\mathfrak{P}_1$ the prime ideal of $B_1$ in $\mathfrak{B}_1$, and let $\Sigma_1^*$ be the residue field $\mathfrak{B}_1/\mathfrak{P}_1$ of $B_1$. The ring $\mathfrak{B}_1$ consists of all those elements of $\Sigma$ whose value in $B$ is either in $\Gamma_1$ or positive, whence $\mathfrak{B}_1 \supset \mathfrak{B}$. $\mathfrak{P}_1$ consists of those elements of $\Sigma$ whose value in $B$ is a positive element of $\Gamma$, not in $\Gamma_1$, whence $\mathfrak{P}_1 \subset \mathfrak{P}$. In particular, the value in $B$ of every element of $\mathfrak{B}_1$ which is not in $\mathfrak{P}_1$, is an element of $\Gamma_1$. There is thus defined an homomorphic mapping of $\Sigma_1^* = \mathfrak{B}_1/\mathfrak{P}_1$ upon the ordered group $\Gamma_1$ of rank 1, i.e. a valuation $B_1^*$ of the field $\Sigma_1^*$, of rank 1. Consequently $\Sigma_1^*$ must be of degree of transcendency 1, since if it was an algebraic extension of $K^*(\cong K)$, it could not possess non-trivial valuation. We conclude that $B_1$ is a 1-dimensional valuation of $\Sigma$, and hence $\Delta_1$ is discrete, of rank 1. Since $\Sigma_1^*$ is of degree of transcendency 1, its valuation $B_1^*$ must be discrete, of rank 1. Hence $\Gamma$ *is a discrete group.* The given valuation $B$ is thus composed of a 1-dimensional valuation $B_1$ of $\Sigma$ (a *divisor* of $\Sigma$), followed up by a valuation $B_1^*$ of the residue field $\Sigma_1^*$ of $B_1$. This field $\Sigma_1^*$ is a field of algebraic functions of one variable and $B_1^*$ is given by a "place", or a "prime divisor" of $\Sigma_1^*$. *The given valuation B is thus defined by a branch of an algebraic curve lying on a normal model of our field.*

The actual association of values in $\Gamma$ to elements in $\Sigma$ is obtained as follows. We fix again an integrally closed finite domain of integrity $\mathfrak{o}$ in $\Sigma$, such that the prime ideal $\mathfrak{p}$ of $B_1$ in $\mathfrak{o}$ be 1-dimensional. In $\mathfrak{o}$ we fix an element $\omega$, such that $\omega \equiv 0(\mathfrak{p}), \omega \not\equiv 0(\mathfrak{p}^{(2)})$. Given any element $\xi$ in $\Sigma$, we can put it in the form $\xi = \omega^m \cdot \alpha/\beta$, where $\alpha, \beta \subset \mathfrak{o}$ and $\alpha \not\equiv 0(\mathfrak{p}), \beta \not\equiv 0(\mathfrak{p})$. Let $(\alpha^*/\beta^*) \neq 0, \infty$ be the element in the residue field $\Sigma_1^*$ which corresponds to $\alpha/\beta$. Let $v_{B_1^*}(\alpha^*/\beta^*) = n$. Then we put $v(\xi) = (m, n)$. The value group $\Gamma$ is the group of all pairs of integers $(m, n)$ ordered lexicographically: $(m, n) < (m_1, n_1)$, if $m_1 > m$ or if $m_1 = m, n_1 > n$. The isolated group $\Gamma_1$ consists of the elements $(0, n)$, $n$-arbitrary. Note that the integer $n$ depends on the choice of the element $\omega$ (except when $m = 0$), but that $m$ is independent on $\omega$. If we choose another element $\omega'$ instead of $\omega$, and if in the original construction the value of $\omega'$ is $(1, \nu)$, $(\nu \gtreqless 0)$, then using $\omega'$ instead of $\omega$, we will get for the value of the same element $\xi$ the pair of integers $(m', n')$, where $m = m', n = \nu m' + n'$. This unimodular transformation defines an order preserving automorphism of $\Gamma$.

### 5. Discrete zero-dimensional valuations of rank 1

The value group $\Gamma$ is the group of all rational integers. Consider an element $\xi$ of $\Sigma$ such that $v(\xi) = +1$. If $\eta$ is any element of $\Sigma$ and if $v(\eta) = \nu$, then $v(\eta/\xi^\nu) = 0$. Since the residue field $\Sigma^*$ is simply isomorphic to the field of constants, it follows that there exists a uniquely determined element $c$ in $\mathsf{K}$ such that $v(\eta/\xi^\nu - c) > 0$, whence

$$\eta = c\xi^\nu + \eta_1, \quad \text{where} \quad v(\eta_1) = \nu_1 > \nu.$$

Applying the same procedure to $\eta_1$ and repeating indefinitely this construction, we get a uniquely determined power series expansion for $\eta$:

$$\eta \to c\xi^\nu + c_1\xi^{\nu_1} + \cdots, \qquad \nu < \nu_1 < \cdots. \tag{2}$$

This defines an *isomorphic* mapping of $\Sigma$ upon a subfield of the field $\mathsf{K}(\{\xi\})$ of integral power series of $\xi$ with coefficients in $\mathsf{K}$. Consider a projective model $V_2$ of the surface, in some $S_n$ $(x_1, \cdots x_n)$, and let $\omega_1, \cdots, \omega_n$ be the coordinates of the general point of $V_2$; $\omega_1, \cdots, \omega_n \subset \Sigma$. We assume that the $\omega$'s are in the valuation ring of $B$. Let

$$\omega_i \to c_{i0} + c_{i1}\xi + c_{i2}\xi^2 + \cdots = \omega_i(\xi).$$

These equations represent an analytical arc $\gamma$ on $V_2$, $x_i = c_{i0} + c_{i1}\xi + \cdots$, whose origin is the point $(c_{10}, \cdots, c_{n0})$. *This arc is not algebraic.* In fact, if $F(\omega_1, \cdots, \omega_n)$ is a polynomial which does not vanish in $\Sigma$, i.e., if $F(x_1, \cdots, x_n)$ does not vanish on $V_2$, then $F(\omega_1, \cdots, \omega_n)$ has a definite value $\mu$ in $B$, and $\xi^\mu$ must be the leading term in the power series $F(\omega_1(\xi), \cdots, \omega_n(\xi))$. In other words, $F(\omega_1(\xi), \cdots, \omega_n(\xi)) \not\equiv 0$ in $\mathsf{K}(\{\xi\})$, if $F(\omega_1, \cdots, \omega_n) \not\equiv 0$ in $\Sigma$ (*isomorphism of the mapping* (2)). Thus $\gamma$ does not lie on any algebraic variety of $S_n$ which does not pass through the surface $V_2$. This proves that $\gamma$ is not an arc of an algebraic curve.

### 6. Non-discrete zero-dimensional valuations of rank 1

Here one is led to distinguish between two cases: (1) the value group $\Gamma$, which may be assumed to be a subgroup of the set of all real numbers, contains at least two incommensurable numbers; (2) any two numbers in $\Gamma$ are commensurable, whence the elements of $\Gamma$ may be assumed to be rational numbers

First Case. Let $x$ and $y$ be two elements whose values $v(x)$ and $v(y)$ are positive incommensurable numbers. We may normalize $\Gamma$ in such a manner that $v(x)$ is equal to 1. Then $v(y) = \tau$, a positive irrational number. Consider any polynomial in $x$ and $y$, say $F(x, y) = \sum a_{ij}x^iy^j$. We have $v(x^iy^j) = i + j\tau$, and, moreover, two distinct terms $a_{ij}x^iy^j$, $a_{i'j'}x^{i'}y^{j'}$ have distinct values, since $i + j\tau = i' + j'\tau$ implies $i = i'$, $j = j'$. If then $a_{\alpha\beta}x^\alpha y^\beta$ is *the* term in $F$ of smallest possible value, then $v(F) = \alpha + \beta\tau$. This implies in the first place

that $x$ *and* $y$ *are algebraically independent*, whence $\Sigma$ is an algebraic extension of the field $\Sigma_1 = \mathsf{K}(x, y)$. In the second place, the value group $\Gamma_1$ of the valuation $B_1$ induced by $B$ in $\Sigma_1$ *is the group of all real numbers of the form* $\alpha + \beta\tau$, $\alpha$ and $\beta$—arbitrary integers.

We know that a fixed multiple of any element $\gamma$ in $\Gamma$ is in $\Gamma_1$, i.e., we have $\nu\gamma = \alpha + \beta\tau$, $\nu$ — a fixed integer. By well known theorem on abelian groups with a finite set of generators, it follows that $\Gamma$ is generated by two elements, say $\delta_1 = r_1 + s_1\tau$, $\delta_2 = r_2 + s_2\tau$, where $r_1$, $s_1$, $r_2$, $s_2$ are rational numbers. Every element in $\Gamma$ is of the form $\alpha\delta_1 + \beta\delta_2$, $\alpha$, $\beta$—integers. We may divide each element in $\Gamma$ by $\delta_1$ and we may thus assert that also $\Gamma$ *is generated by the two elements* 1, $\tau^* = \delta_2/\delta_1$, *where* $\tau^*$ *is clearly an irrational number.* Thus $\Gamma$ is of the same type as $\Gamma_1$.

The induced valuation $B_1$ in $\mathsf{K}(x, y)$ can be obtained by putting formally $y = x^\tau$. Then for any polynomial $f(x, y) = \sum a_{ij}x^iy^j$ we find: $v(f) = \min\{i + j\tau\}$. The equation $y = x^\tau$ may be regarded as representing a *transcendental branch* in the $(x, y)$-plane.[7] If we take as a projective model of $\Sigma$ a surface $F$ in an $(x, y, z)$-space, then the valuation $B$ is represented on $F$ by one of the transcendental branches whose projection onto the $(x, y)$-plane is the branch $y = x^\tau$.

Second Case. The elements of $\Gamma$ are in this case rational numbers. The denominators must be arbitrarily high, since $\Gamma$ is not discrete. We consider the prime numbers which occur in the denominators of the various elements $m/n$ of $\Gamma$, where we assume that each quotient is written in its lowest terms. We distribute these prime numbers into two classes: in the first class, say $\{p\}$, we put those prime numbers $p_1, p_2, \cdots$ which occur in the denominators $n$ only to a bounded power, say $p_i$ occurs to the power $\nu_i$ but not to the power $\nu_i + 1$; in the second class, which we shall denote by $\{q\}$, we put the prime numbers $q_1, q_2, \cdots$ which occur in the denominators $n$ to an arbitrarily high power. Any one of the two sets $\{p\}$ $\{q\}$ may contain a finite or infinite set of elements, or may be vacuous. However, if $\{q\}$ is vacuous, then necessarily the set $\{p\}$ must contain an infinity of prime numbers. We may assume that $\Gamma$ contains the number 1.

*We assert then that* $\Gamma$ *consists of all the rational numbers whose denominators are of the form* $p_1^{m_1}p_2^{m_2}\cdots q_1^{n_1}q_2^{n_2}\cdots$, $m_1 \leqq \nu_1$, $m_2 \leqq \nu_2, \cdots, n_1, n_2, \cdots$— *arbitrary integers.* This assertion follows from the following two remarks.

*First*: if $\Gamma$ contains a rational number $a = \alpha/\beta$, $(\alpha, \beta) = 1$, then $\Gamma$ contains

---

[7] A suggestive geometric interpretation can be given by using the theory of infinitely near points. Let $f_i/g_i$, $i = 1, 2, \cdots$, be the convergent fractions of the infinite continued fraction for $\tau$. On the *algebraic branch* $y = x^{f_i/g_i}$ we find a set $M_i$ of infinitely near points $A_1, A_2, \cdots, A_{\sigma_i}$, consisting of a set of free points, followed by a set of satellites (see Enriques-Chisin, *Teoria geometrica delle equazioni e delle curve algebriche*, Vol. II). Moreover, it is well known that the set $M_i$ is a subset of $M_{i+1}$. The branch $y = x^\tau$ may be associated with the infinite sequence $\{A_1, A_2, \cdots, A_m, \cdots\} = \lim M_i$, of infinitely near points.

$1/\beta$ (and hence all its multiples). In fact, let $m\alpha + n\beta = 1$. Then $1/\beta = m\alpha + n$.

*Second*: if $\Gamma$ contains $a = \alpha/\beta$ and $a_1 = \alpha_1/\beta_1$, $(\alpha, \beta) = 1$, $(\alpha_1, \beta_1) = 1$, and if $(\beta, \beta_1) = 1$, then $\Gamma$ contains $1/\beta\beta_1$. In fact, $a + a_1 = (\alpha\beta_1 + \alpha_1\beta)/\beta\beta_1$. Clearly $\alpha\beta_1 + \alpha_1\beta$ and $\beta\beta_1$ are relatively prime, and our assertion follows from the first remark.

For the actual construction of valuations of this type we proceed as follows. We consider two algebraically independent elements $x$ and $y$ in $\Sigma$, contained in the prime ideal of the valuation. We may assign to $x$ the value 1. We pass to the complete field $\Omega$ relative to the given valuation $B$, and containing the field $\Sigma$. In $\Omega$ we have an extended valuation with the same value group $\Gamma$ as $B$ and with the same residue field $\mathsf{K}$. Moreover, every convergent sequence of elements in $\Omega$ has a limit in $\Omega$. It is well known that $\Omega$ is simply isomorphic to a subfield of the field $\mathsf{K}(\{x\})_\Gamma$ of all well ordered power series in $x$ with coefficients in $\mathsf{K}$ and exponents in $\Gamma$. Hence we have for $y$ an expansion of the form:

$$(3)\quad y = c_1x^{m_1/n_1} + c_2x^{m_2/n_2} + c_3x^{m_3/n_3} + \cdots, \qquad \frac{m_1}{n_1} < \frac{m_2}{n_2} < \frac{m_3}{n_3} < \cdots,$$

each $m_i/n_i$ being a rational number in its lowest terms. We have exhibited in (3) only the simple power series (of type $\omega$) with which the well ordered series begins. It is not difficult to see that by substituting the above simple power series for $y$ into any given rational function $\eta$ of $x$ and $y$ we get a power series in $x$ such that the value of $\eta$ is the exponent of the leading term of the series.[8] By a simple Puiseux argument (see Schilling,[7] p. 702) it is not difficult to show that any of the denominators $n_i$ in the exponents actually occurs as a denominator in some element of the value group. Since we may assign the expansion (3) arbitrarily, it follows that any subgroup of the group of rationals is the value group of some valuation of $\Sigma$.

## II. Uniformization of Valuations. The Fundamental Lemma

### 7.

Let $B$ be a zero-dimensional valuation of our field $\Sigma$. Given any set of elements $\xi_1, \cdots, \xi_n$ which generate the field $\Sigma$, there is defined a surface $F$ in $S_n$, whose general point has coördinates $\xi_1, \cdots, \xi_n$ and which is a projective model of $\Sigma$. If the $\xi$'s are in the valuation ring of $B$, and if, say, $\xi_i - c_i$, $c_i \subset \mathsf{K}$, has positive value in $B$, then the prime ideal of $B$ in the ring $\mathsf{K}[\xi_1, \cdots, \xi_n]$ is the zero-dimensional ideal $(\xi_1 - c_1, \cdots, \xi_n - c_n)$. The valuation $B$ is then defined by a branch on the surface $F$, algebraic, analytical, or transcendental, through the point $A(c_1, \cdots, c_n)$. We shall call this point *the center of the valuation* on $F$.

[8] The substitution may actually lead to a well ordered series of type $> \omega$. However, we associate with $\eta$ the simple power series with which the well ordered series begins.

FUNDAMENTAL LEMMA. *Given any zero-dimensional valuation $B$ of the field $\Sigma$, there exists a projective model $F$ of $\Sigma$, on which the center of the valuation $B$ is at a simple point of the surface.*

In the proof of this theorem we have to consider separately the various types of valuations as classified in the preceding sections.

### A. VALUATIONS OF RANK 2 (ALGEBRAIC BRANCHES)

Let $B_1$ be the one-dimensional valuation with which $B$ is composed. We choose two independent elements $x$ and $y$ in $\Sigma$ such that the prime ideal of $B_1$ in the ring $\mathfrak{o}$ of integral functions of $x$, $y$ be one-dimensional ($B_1$—a divisor of the first kind with respect to the ring $\mathfrak{o}$). Let $\mathfrak{p}_1$ be this prime ideal.

Let $x_1$, $y_1$ be any other two elements in $\mathfrak{o}$, such that $\mathfrak{o}$ is the integral closure of $\mathsf{K}[x_1, y_1]$, and let $z$ be a primitive element of $\Sigma$ with respect to the field $\mathsf{K}(x_1, y_1)$. Let $f(x_1, y_1, z) = 0$ be the irreducible equation for $z$, over $\mathsf{K}(x_1, y_1)$. We have shown in $Z_2$ that there always exist elements $x_1$, $y_1$, $z$ such that $f'_z(x_1, y_1, z) \not\equiv 0(\mathfrak{p}_1)$.[9] We shall assume that the original elements $x$, $y$ are the $x_1$ and $y_1$ respectively. We have then

$$f(x, y, z) = 0 \tag{4}$$

$$f'_z(x, y, z) \not\equiv 0(\mathfrak{p}_1). \tag{4'}$$

The relation (4') implies that the *value of the element $f'_z(x, y, z)$ in our valuation $B$ is of the form* $(0, n)$. This remark is of decisive importance.

We consider the surface $F$ defined by (4) in $S_3(x, y, z)$. It is a projective model of our field $\Sigma$. On $F$ our valuation $B$ gives rise to an algebraic branch $\gamma$. We may assume that the origin of this branch is the point $O$: $x = y = z = 0$. Let us suppose that $O$ is a multiple point, say an $r$-fold point, $r > 1$. Then $f(x, y, z)$ is of the form

$$f = f_r + f_{r+1} + \cdots + f_m,$$

where $f_i = f_i(x, y, z)$ is a form of degree $i$. The elements $x$, $y$, $z$ have positive values in $B$. We shall have to arrange $x$, $y$, $z$ in an order corresponding to the order of magnitude of their values. To avoid the necessity of considering various cases, we present the relation (4') in such a form that will make the element $z$ lose its privileged rôle. Namely, let us consider the three partial derivatives $f'_x$, $f'_y$, $f'_z$, and let us write that

$$\min\,(v(f'_x), v(f'_y), v(f'_z)) = (0, n),$$

without specifying which of the three derivatives has the minimum value $(0,n)$. The point $O$ is a multiple point of $F$ if and only if $n > 0$. Now it is clear that we may assume, without loss of generality:

$$0 < v(x) \leqq v(y) \leqq v(z).$$

[9] This assertion is equivalent with theorem 11 (section 16) of the quoted paper, to the effect that the normal surfaces defined by the integrally closed ring $\mathfrak{o}$ do not possess *multiple curves*. See also theorem 4 (section 5), loc. cit.

Since $B$ is zero-dimensional, there exist uniquely determined constants $c$, $d$ such that $v(y - cx) > v(x)$, $v(z - cx) > v(x)$. We apply to $F$ the quadratic transformation

$$x_1 = x, \qquad y_1 = \frac{y - cx}{x}, \qquad z_1 = \frac{z - dx}{x}, \tag{5}$$

whose inverse is given by the formulas:

$$x = x_1, \qquad y = x_1(y_1 + c), \qquad z = x_1(z_1 + d).$$

Substituting into the equation $f(x, y, z) = 0$ we get

$$f(x, y, z) = x_1^r f_1(x_1, y_1, z_1),$$

where

$$f_1(x_1, y_1, z_1) = f_r(1, y_1, z_1) + x_1 f_{r+1}(1, y_1, z_1) + \cdots + x_1^{m-r} f_m(1, y_1, z).$$

Denote by $F_1$ the transformed surface

$$f_1(x_1, y_1, z_1) = 0.$$

By (5), the values of $x_1$, $y_1$, $z_1$ in $B$ are positive. Hence $B$ is given on $F_1$ by a branch through the origin $x_1 = y_1 = z_1 = 0$. We find immediately the following relations:

$$f'_x = x_1^{r-1}\{x_1 f'_{1x_1} - (y_1 + c)f'_{1y_1} - (z_1 + d)f'_{1z_1}\}$$

$$f'_y = x_1^{r-1} \cdot f'_{1y_1}$$

$$f'_z = x^{r-1} f'_{1z_1}.$$

Hence

$$\min (v(f'_x), v(f'_y), v(f'_z)) \geqq (r - 1)v(x_1) + \min (v(f'_{1x_1}), v(f'_{1y_1}), v(f'_{1z_1})).$$

By assumption $O$ is a multiple point of $F$, i.e. $r \geqq 2$. Since $v(x_1) > 0$, we conclude that

$$\min (v(f'_{1x_1}), v(f'_{1y_1}), v(f'_{1z_1})) = (0, n_1) < (0, n),$$

whence $0 < n_1 < n$.

If the origin $x_1 = y_1 = z_1 = 0$, the center of the valuation $B$ on $F_1$, is still a multiple point, we apply to this surface a new quadratic transformation, getting a new surface

$$f_2(x_2, y_2, z_2) = 0,$$

on which the valuation $B$ is represented by a branch through the point $x_2 = y_2 = z_2 = 0$, and we will also have

$$\min (v(f'_{2x_2}), v(f'_{2y_2}), v(f'_{2z_2})) = (0, n_2), \qquad n > n_1 > n_2 > 0.$$

It follows that after a finite number of steps we will get a surface

$$f_i(x_i, y_i, z_i) = 0,$$

such that at least one of the 3 partial derivatives $f_{ix_i}$, $f_{iy_i}$, $f_{iz_i}$ has *value zero*, (i.e. (0, 0)), in the given valuation $B$. That implies, that on the surface $f_i = 0$, the center of our valuation $B$ is a point at which not all the partial derivatives of $f_i$ vanish. This point is therefore a simple point of the surface $f_i = 0$.

### B. Discrete Valuations of Rank 1 (Analytical Branches)

The proof in this case is identical with the proof in the preceding case, and even simpler, since now, because of the archimedean character of the value group, the value of any element in $\Sigma$, different from zero, is an integer. Hence in the present case it is permissible to begin with an *arbitrary* projective model $f(x, y, z) = 0$ of $\Sigma$, whereas in the preceding case we had to be careful with our choice of this model, because we wished to satisfy the minimum value requirement for the partial derivatives (i.e. that this minimum be a pair of integers $(m, n)$ in which $m = 0$).

### C. Non-Discrete Valuations of Rank 1 (Transcendental Branches)

**8. First case. The value group consists of all elements of the form $m + n\tau$, $m, n$—integers, $\tau$—an irrational number**

We choose two elements $x$ and $y$ in $\Sigma$ such that $v(x) = 1$, $v(y) = \tau$. Then $x$ and $y$ are algebraically independent. Let $z$ be an element whose value is positive and which is a primitive element of $\Sigma$ with respect to the field $\mathsf{K}(x, y)$, and let

$$f(x, y, z) = 0$$

be the corresponding projective model $F$ of $\Sigma$. Our valuation is then represented on the surface $F$ by a branch through the origin. Our proof will be essentially a suitably modified Puiseux argument.

Since $f(x, y, z)$ is the element zero of $\Sigma$, there must exist two or more terms in the polynomial $f(x, y, z)$ which have equal and minimum value. If two distinct terms $x^i y^j z^\nu$, $x^{i_1} y^{j_1} z^{\nu_1}$ have equal value, then necessarily $\nu \neq \nu_1$. In fact, if $\nu = \nu_1$, then $v(x^i y^j) = v(x^{i_1} y^{j_1})$, i.e. $i + j\tau = i_1 + j_1\tau$, whence $i = i_1$, $j = j_1$. We arrange then the minimum value terms according to increasing powers of $z$ and we write:

$$f(x, y, z) = a_\alpha x^{m_\alpha} y^{n_\alpha} z^\alpha + a_\beta x^{m_\beta} y^{n_\beta} z^\beta + \cdots + a_\delta x^{m_\delta} y^{n_\delta} z^\delta + \Sigma' a_i x^{m_i} y^{n_i} z^{l_i},$$
$$\alpha < \beta < \cdots < \delta,$$

where

$$M + N\tau = v(x^{m_\alpha} y^{n_\alpha} z^\alpha) = \cdots = v(x^{m_\beta} y^{n_\beta} z^\beta) = \cdots = v(a_\delta x^{m_\delta} y^{n_\delta} z^\delta),$$

and where the summation $\Sigma'$ is extended to all remaining terms whose value is $> M + N\tau$. Here

$$M = m_\alpha + s\alpha = m_\beta + s\beta = \cdots = m_\delta + s\delta,$$
$$N = n_\alpha + \sigma\alpha = n_\beta + \sigma\beta = \cdots = n_\delta + \sigma\delta,$$

and

$$v(z) = s + \sigma\tau, \qquad s, \sigma\text{—integers} \gtreqless 0.$$

Moreover,

$$(m_i + l_i s) + (n_i + l_i\sigma)\tau > M + N\tau, \tag{6}$$

for any term in the sum $\Sigma'$.

We may assume that $f(0, 0, z)$ is not identically zero in $z$ (i.e. that the $z$-axis does not lie on the surface $F$). Let $z = 0$ be an $r$-fold root of $f(0, 0, z)$. If $r = 1$, the origin—center of the valuation—is a simple point of $F$. Assume $r > 1$. Then $f(x, y, z)$ contains the terms $az^r$, $a \subset K$. Since we must have $v(x^{m_i}y^{n_i}z^{l_i}) \leqq v(z^r)$, it follows that

$$\delta \leqq r. \tag{7}$$

We expand $\tau$ into a continued fraction:

$$\tau = h_1 + \cfrac{1}{h_2 + \cfrac{1}{h_3 + \cdots}}.$$

Let $f_j/g_j$ be the convergent fractions of $\tau$. Since $\lim f_j/g_j = \tau$, we can find an integer $p$, sufficiently high, such that the inequalities (6) remain true if $\tau$ is replaced by $f_{p-1}/g_{p-1}$ and also by $f_p/g_p$. We will have then

$$(m_i + l_i s) + (n_i + l_i\sigma)\cdot f_j/g_j > M + N\cdot f_j/g_j, \quad j = p - 1, p, \tag{6'}$$

for any term $a_i x^{m_i}y^{n_i}z^{l_i}$ which is not a minimum value term.

We now pass from the elements $x, y, z$ of $\Sigma$ to new elements $x_1, y_1, z_1$ by the following Cremona transformation:

$$x = x_1^{g_p}y_1^{g_{p-1}}, \qquad y = x_1^{f_p}y_1^{f_{p-1}}, \qquad z = x^s y^\sigma(z_1 + c). \tag{8}$$

Here $c$ is a constant determined as follows: since $v(z) = s + \sigma\tau = v(x^s y^\sigma)$, it follows that $v(z/x^s y^\sigma) = 0$. There exists then a uniquely determined constant $c$ such

$$v(z_1) = v\left(\frac{z}{x^s y^\sigma} - c\right) > 0, \qquad c \neq 0. \tag{9}$$

By known properties of convergent fractions we have

$$f_{p-1}g_p - f_p g_{p-1} = \epsilon = \pm 1.$$

We also know that $\epsilon$, $-\tau + f_{p-1}/g_{p-1}$ and $\tau - f_p/g_p$ have like signs. From (8) we find

$$x_1^\epsilon = x^{f_{p-1}}/y^{g_{p-1}}, \qquad y_1^\epsilon = y^{g_p}/x^{f_p},$$

whence

$$\epsilon v(x_1) = g_{p-1}\left(\frac{f_{p-1}}{g_{p-1}} - \tau\right), \qquad \epsilon v(y_1) = g_p\left(\tau - \frac{f_p}{g_p}\right).$$

Hence

(9′) $\quad v(x_1) > 0, \quad v(y_1) > 0, \quad$ and also $\quad v(z_1) > 0$, by (9).

By our transformation (8) every minimum value term in the equation $f(x, y, z) = 0$ acquires *the same factor*

$$x_1^{Mg_p+Nf_p} y_1^{Mg_{p-1}+Nf_{p-1}},$$

while, in view of (6′), every other term acquires a factor $x_1^{\lambda_i} y_1^{\mu_i}$, where $\lambda_i > Mg_p + Nf_p$, $\mu_i > Mg_{p-1} + Nf_{p-1}$. Hence

$$f(x, y, z) = x_1^{Mg_p+Nf_p} y_1^{Mg_{p-1}+Nf_{p-1}} \cdot f_1(x_1, y_1, z_1),$$

where

$$f_1(x_1, y_1, z_1) = 0$$

is the equation of the transformed surface $F_1$, and $f_1$ has the form

$$f_1(x_1, y_1, z_1) = (z_1 + c)^\alpha \{a_\alpha + a_\beta(z_1 + c)^{\beta-\alpha} + \cdots a_\delta(z_1 + c)^{\delta-\alpha}\} + x_1 y_1 H(x_1, y_1, z_1).$$

Since the center of our valuation $B$ on the new surface $F_1$ is at the origin $x_1 = y_1 = z_1 = 0$ (in view of (9′)), we must have $f(0, 0, 0) = 0$, whence $u = c$ must be a root of the polynomial $\phi(u) = a_\alpha + a_\beta u^{\beta-\alpha} + \cdots + a_\delta u^{\delta-\alpha}$. Let $c$ be an $r_1$-fold of this polynomial. Then $z_1 = 0$ is an $r_1$-fold root of $f(0, 0, z_1)$. We have

$$r_1 \leqq \delta - \alpha \leqq r, \text{ by (7).}$$

If $r_1 < r$, we have achieved a reduction, since for $r = 1$ we get a simple point. Assume that $r_1 = r$. This implies that $\alpha = 0$, $\delta = r$ and that $\phi(u) = a_0 + a_\beta u^\beta + \cdots + a_r u^r = a_r(u - c)^r$. Hence the minimum value terms of $f(x, y, z)$ have the form

$$a_0 x^{m_0} y^{n_0} + a_1 x^{m_1} y^{n_1} z + \cdots + a_{r-1} x^{m_{r-1}} y^{n_{r-1}} z^{r-1} + a_r z^r,$$

where $a_{r-1} \neq 0$, $a_r \neq 0$. Since $v(z^r) = v(x^{m_{r-1}} y^{n_{r-1}} z^{r-1})$, it follows that

$$v(z) = m_{r-1} + n_{r-1} \cdot \tau.$$

We express this conclusion as follows: *if our transformation from* $f(x, y, z) = 0$ to $f_1(x_1, y_1, z_1) = 0$ *does not reduce the value of* $r$, *then the value of* $z$ *in* $B$ *is of the form* $m + n\tau$, *where* $m$ *and* $n$ *are non-negative integers.*

Let then $v(z) = m + n\tau > 0$, $m, n \geqq 0$. There exist then a uniquely determined constant $c$ such that $v(z - cx^m y^n) > v(z)$. Let

$$z = cx^m y^n + z_1, \qquad v(z_1) > v(z),$$

$$f(x, y, z) = f(x, y, cx^m y^n + z_1) = f_1(x, y, z_1) = 0.$$

Clearly $z_1 = 0$ is also an $r$-fold root of $f_1(0, 0, z_1)$. We can apply a transformation such as (8) to the new surface $f_1 = 0$. If there is again no reduction as far as $r$ is concerned, then also the value of $z_1$ in $B$ must be of the form

$$v(z_1) = m_1 + n_1\tau,\ m_1, n_1 \geqq 0.$$

We then put

$$z_1 = c_1 x^{m_1} y^{n_1} + z_2,$$

where the constant $c_1$ is determined in such a fashion that $v(z_2) > v(z_1)$. We get a new surface $F_2$ :

$$f_2(x, y, z_2) = f_1(x, y, c_1 x^{m_1} y^{n_1} + z_2) = 0.$$

Suppose that we get in this fashion a sequence of birational transforms of our surface $f(x, y, z) = 0$:

$$f_i(x, y, z_i) = 0, \qquad i = 0, 1, \cdots, f_0 = f, \qquad z_0 = z,$$

such that $z_i = 0$ is always also an $r$-fold root of $f_i(0, 0, z_i)$ and such that our Cremona transformation, of type (8), if applied to the surface $f_i = 0$ is not capable of reducing the value of $r$. Here

$$z_i = c_i x^{m_i} y^{n_i} + z_{i+1},$$

$$v(z_{i+1}) = m_{i+1} + n_{i+1}\tau > m_i + n_i\tau = v(z_i) > 0,$$

and $m_i$, $n_i$ are non-negative integers.

Now

$$f_{i+1}(x, y, z_{i+1}) = f_i(x, y, c_i x^{m_i} y^{n_i} + z_{i+1}),$$

whence

$$\frac{\partial f_{i+1}}{\partial z_{i+1}} = \frac{\partial f_i}{\partial z_i}. \tag{10}$$

Since in each polynomial $f_i$ the term in $z_i^r$ must be among the minimum value terms, it follows that

$$v\left(\frac{\partial f_i}{\partial z_i}\right) \geqq (r-1)v(z_i),$$

or, since $r > 1$,

$$v\left(\frac{\partial f_i}{\partial z_i}\right) \geqq v(z_i).$$

In view of (10) it follows that

$$v\left(\frac{\partial f}{\partial z}\right) \geqq m_i + n_i\tau. \tag{11}$$

Now if our sequence of surfaces $f_i = 0$ was infinite, we would have an infinite ascending sequence of real numbers

$$0 < m + n\tau < m_1 + n_1\tau < \cdots < m_i + n_i\tau < \cdots,$$

whose limit is $+\infty$, *since the integers* $m_i$, $n_i$ *are non-negative.* This is in contradiction with the inequality (11), since $\partial f/\partial z \not\equiv 0$ in $\Sigma$ ($f$ being irreducible). Thus, after a finite number of steps we must get a surface $f_i(x, y, z_i) = 0$ such that a Cremona transformation of type (8), applied to the surface, diminishes the value of $r$. Ultimately we get a surface for which $r = 1$, and on that surface the center of our valuation is at a simple point.

### 9. Second case. The value group consists of rational numbers

We choose arbitrarily two algebraically independent elements $x$ and $y$ in $\Sigma$. Let

$$\frac{v(y)}{v(x)} = \frac{\mu}{\nu}, \qquad (\mu, \nu) = 1$$

and let $\mu'$, $\nu'$ be positive integers such that

$$\mu'\nu - \mu\nu' = +1.$$

We define a Cremona plane transformation $C_1$ as follows:

$$C_1\colon\ x = x_1^{\nu}(y_1 + c_1)^{\nu'}, \qquad y = x_1^{\mu}(y_1 + c_1)^{\mu'},$$

where $c_1$ is a constant still to be determined.

For $C_1^{-1}$ we find the equations:

$$C_1^{-1}\colon x_1 = x^{\mu'}/y^{\nu'}, \qquad (y_1 + c_1) = y^{\nu}/x^{\mu}.$$

From these equations it follows in the first place that

$$v(x_1) = \mu' \cdot v(x) - \nu' v(y) = \frac{v(x)}{\nu}(\mu'\nu - \nu'\mu) = \frac{v(x)}{\nu} > 0.$$

Moreover, since $v(y^{\nu}/x^{\mu}) = 0$, also $v(y_1 + c_1) = 0$. We choose the constant $c_1$ in such a fashion that $v(y_1) > 0$. We have now two new elements $x_1$, $y_1$ whose values are positive.

In a similar fashion we define a plane Cremona transformation $C_2$ from the $(x_1, y_1)$ plane to a $(x_2, y_2)$ plane, where again $v(x_2) > 0$, $v(y_2) > 0$:

$$C_2\colon\ x_1 = x_2^{\nu_1}(y_2 + c_2)^{\nu_1'}, \qquad y_1 = x_2^{\mu_1}(y_2 + c_2)^{\mu_1'},$$

where

$$\frac{v(y_1)}{v(x_1)} = \frac{\mu_1}{\nu_1}, \qquad (\mu_1, \nu_1) = 1 \quad \text{and} \quad \mu_1'\nu_1 - \mu_1\nu_1' = +1.$$

We get a sequence of Cremona transformations:

$$T_1 = C_1, \qquad T_2 = C_1C_2, \cdots, T_i = C_1C_2 \cdots C_i, \cdots,$$

where $T_i$ is a transformation leading to elements $x_i$, $y_i$. The elements $x$, $y$ are polynomials in $x_i$, $y_i$.

We prove the following

LEMMA. *Given a polynomial $\phi(x, y)$, then for all sufficiently high values of $i$ the expression of $\phi(x, y)$ as a polynomial in $x_i$, $y_i$ is of the form*

$$\phi(x, y) = x_i^{\lambda_i}\phi^{(i)}(x_i, y_i), \qquad \lambda_i \geqq 0,$$

*where* $\phi^{(i)}(0, 0) \neq 0$.

The proof of this lemma is essentially the classical Puiseux argument. We put into evidence the minimum value terms in $\phi(x, y)$:

$$\phi(x, y) = a_\alpha x^{m_\alpha}y^\alpha + a_\beta x^{m_\beta}y^\beta + a_\delta x^{m_\delta}y^\delta + \sum{}' a_i x^{m_i}y^{l_i}, \quad \alpha < \beta < \cdots < \delta,$$

where

$$m_\alpha\nu + \alpha\mu = m_\beta\nu + \beta\mu = \cdots = m_\delta\nu + \delta\mu = \rho$$

and

$$m_i\nu + l_i\mu > \rho$$

for all remaining terms.

Applying the transformation $C_1$ we find

$$\phi(x, y) = x_1^\rho\phi_1(x_1, y_1),$$

where

$$\phi_1(x_1, y_1) = a_\alpha(y_1 + c_1)^{m_\alpha\nu' + \alpha\mu'} + a_\beta(y_1 + c_1)^{m_\beta\nu' + \beta\mu'} + \cdots + a_\delta(y_1 + c_1)^{m_\delta\nu' + \delta\mu'} + x_1H(x_1, y_1),$$

or

$$\phi_1(x_1, y_1) = (y_1 + c_1)^{m_\alpha\nu' + \alpha\mu'}\{a_\alpha + a_\beta(y_1 + c_1)^{\frac{\beta-\alpha}{\nu}} + \cdots + a_\delta(y_1 + c_1)^{\frac{\delta-\alpha}{\nu}}\} + x_1H(x_1, y_1).$$

If $u = c_1$ is not a root of the polynomial

$$g(u) = a_\alpha + a_\beta u^{\frac{\beta-\alpha}{\nu}} + \cdots + a_\delta u^{\frac{\delta-\alpha}{\nu}},$$

then $\phi_1(0, 0) \neq 0$, and our lemma is proved.

If $g(c_1) = 0$, then our transformation $C_1$ has the same effect as the classical Puiseux substitution $x = x_1^\nu$, $y = x_1^\mu(c_1 + y_1)$, used in the determination of the branches of the curve $\phi(x, y) = 0$ passing through the origin $x = y = 0$. The only difference—and advantage—is that our transformation *does not* lead to elements $x_1$, $y_1$ outside the field $\mathsf{K}(x, y)$. The remainder of the proof is now clear. It is sufficient to observe that if our lemma was not true for the given polynomial $\phi(x, y)$, then the above reasoning shows that the valuation $B$ would be the one which is determined by a branch of the curve $\phi(x, y) = 0$ through the origin $x = y = 0$. This is impossible, since $B$ corresponds, by hypothesis, to a transcendental branch.

Let now $z$ be a primitive element of $\Sigma$ over $K(x, y)$ and let $v(z) > 0$. Let $F$ be the surface given the irreducible equation

$$f(x, y, z) = 0.$$

We write $f$ as a polynomial in $z$ and we put into evidence the terms of minimum value:

$$f(x, y, z) = a_\alpha(x, y)z^\alpha + a_\beta(x, y)z^\beta + \cdots + a_\delta(x, y)z^\delta + \sum{}' a_i(x, y)z^i,$$

where

$$v(a_\alpha z^\alpha) = v(a_\beta z^\beta) = \cdots = v(a_\delta z^\delta) \tag{12}$$

and

$$v(a_i z^i) > v(a_\alpha z^\alpha) \text{ for all remaining terms.}$$

The center of our valuation $B$ on the surface $F$ is the origin $x = y = z = 0$. Let, as in the preceding section, $z = 0$ be an $r$-fold root of $f(0, 0, z)$. If $r = 1$, the origin is a simple point. Suppose $r > 1$.

We apply first our Cremona transformation $T_i$ to $x$ and $y$ and we choose $i$ sufficiently high, so that the above lemma be applicable to all the polynomials $a_\alpha, a_\beta, \cdots, a_\delta, a_i$ simultaneously (i.e., to their product). Let us denote the new elements $x_i, y_i$ by $\bar{x}, \bar{y}$. Then $f(x, y, z)$ takes the form:

$$f(x, y, z) = \bar{f}(\bar{x}, \bar{y}, \bar{z}) = \bar{x}^{m_\alpha}\bar{a}_\alpha(\bar{x}, \bar{y})z^\alpha + \bar{x}^{m_\beta}\bar{a}_\beta(\bar{x}, \bar{y})z^\beta + \cdots + \bar{x}^{m_\delta}\bar{a}_\delta(\bar{x}, \bar{y})z^\delta + \sum{}' \bar{x}^{m_i}\bar{a}_i(\bar{x}, \bar{y})z^i,$$

where $\bar{a}_\alpha(0, 0), \bar{a}_\beta(0, 0), \bar{a}_\delta(0, 0), \bar{a}_i(0, 0)$ are all $\neq 0$.

Let now $v(z)/v(\bar{x}) = s/\sigma$, $(s, \sigma) = 1$, and let $s', \sigma'$ be positive integers such that

$$s'\sigma - s\sigma' = +1.$$

We apply to the surface $\bar{f}(\bar{x}, \bar{y}, z) = 0$ the quadratic transformation:

$$\bar{x} = x_1^\sigma(z_1 + c_1)^{\sigma'}, \qquad z = x_1^s(z_1 + c_1)^{s'}, \qquad \bar{y} = y_1,$$

where the constant $c_1$ is $\neq 0$ and is determined by the condition: $v(z_1) > 0$. Let

$$f_1(x_1, y_1, z_1) = 0$$

be the equation of the transformed surface. We find immediately, in view of (12),

$$f(x, y, z) = \bar{x}^{m_\alpha\sigma + \alpha s} f_1(x_1, y_1, z_1),$$

and

$$f_1(x_1, y_1, z_1) = (z_1 + c_1)^{m_\alpha\sigma' + \alpha s'}\{\bar{a}_\alpha(\bar{x}, \bar{y}) + \bar{a}_\beta(\bar{x}, \bar{y})(z_1 + c_1)^{(\beta-\alpha)/\sigma} + \cdots + \bar{a}_\delta(\bar{x}, \bar{y})(z_1 + c_1)^{(\delta-\alpha)/\sigma}\} + x_1 H(x_1, y_1, z_1).$$

Naturally, in view of our choice of the constant $c_1$, we must have $f_1(0, 0, 0) = 0$. As in the preceding section we conclude that the multiplicity of the root $z_1 = 0$

for $f_1(0, 0, z_1)$ is $\leqq r$, and that it equals $r$ if and only if $\alpha = 0$, $\delta = r$ and if $\bar{a}_0(0, 0) + \bar{a}_1(0, 0)u + \cdots + \bar{a}_r(0, 0)u^r = (u - c_1)^r$. The minimum value terms in the original polynomial $f(x, y, z)$ are then the following:

$$a_0(x, y) + a(x, y)z + \cdots + a_{r-1}(x, y)z^{r-1} + a_r(x, y)z^r,$$

where $a_r(0, 0) \neq 0$ (since $f(x, y, z)$ contains a term in $z^r$). As a consequence, $v(z) = v(a_{r-1}(x, y))$, i.e. *the value of $z$ is equal to the value of a polynomial in $x$ and $y$.* This conclusion is altogether parallel to the one reached in the course of the proof given in the preceding section. The only difference is that in the first case the value of $z$ was the value of a power product $x^m y^n$. The remainder of the proof runs along similar lines, as in the first case. If $v(z) = v(a(x, y))$, $a$—a polynomial, we can find a constant $c$ such that $v(z - c \cdot a(x, y)) > v(z)$. We pass to the element $z_1 = z - c \cdot a(x, y)$ and to the surface $f_1(x, y, z_1) = 0$. Repeating this procedure, we get a sequence of surfaces $f_i(x, y, z_i) = 0$, such that

(1) $z_i = 0$ is an $r$-fold root of $f_i(0, 0, z_i)$;
(2) $v(z_i) = v(a_i(x, y))$, $a_i$—a polynomial;
(3) $v(z) < v(z_1) < v(z_2) < \cdots$; $z_{i+1} = z_i - c_i \cdot a_i(x, y)$.

As in the preceding case we conclude with the inequality

$$v\left(\frac{\partial f}{\partial z}\right) \geqq v(a_i),$$

which shows that our sequence of surfaces $f_i$ must be finite, since it is easily seen that *a strictly ascending sequence of real numbers, in which each element is the value of a polynomial, has $+\infty$ as a limit.*[10] This completes the proof of the fundamental lemma.

## III. Ideals in the Quotient Ring of a Simple Point

### 10.

Let $F$ be an algebraic surface in an $S_n$, a projective model of the field $\Sigma$, and let $\xi_1, \cdots, \xi_n$ be the non-homogeneous coördinates of the general point of $F$. In $Z_2$ (section 21) we have associated to every point $P$ of $F$ a *quotient ring* $Q(P)$. Namely, assuming (without loss of generality) that $P$ is a point at finite distance, let $a_1, \cdots a_n$ be its non-homogeneous coördinates. Then $Q(P)$ is the set of all quotients of $f(\xi_1, \cdots, \xi_n)/g(\xi_1, \cdots, \xi_n)$ of polynomials in the $\xi$'s, such that the denominator does not vanish at $P$, i.e. $g(a_1, \cdots, a_n) \neq 0$.

[10] Let $\rho$ be a fixed positive real number and let $0 < \sigma = \min(v(x), v(y))$. Let $n_\rho$ be the smallest integer such that $n_\rho \cdot \sigma > \rho$. Let $g(x, y)$ be a polynomial whose value is not greater than $\rho$. We separate in $g$ the terms of degree $< n_\rho$ from those of degree $\geqq n_\rho$, i.e. we write $g = g' + g''$, where $g'$ is the polynomial of degree $< n_\rho$. Every form in $x$, $y$, of degree $m$, has value $\geqq m\sigma$. Hence $v(g'') \geqq n_\rho\sigma > \rho$. Since $v(g) \leqq \rho$, it follows that $v(g') = v(g)$. Hence, if a polynomial has a value not greater than $\rho$, then its value is the value of some polynomial of degree $< n_\rho$. It follows that among the values assumed by polynomials in $x$, $y$ there is only a finite number of values which are not greater than a given fixed real number $\rho$. This proves our assertion.

If $\mathfrak{J}$ denotes the ring of polynomials $\mathsf{K}[\xi_1, \cdots, \xi_n]$, then (in ideal theoretic language) $Q(P)$ is the quotient ring $\mathfrak{J}^* = \mathfrak{J}_{\mathfrak{p}_0}$ of the prime zero-dimensional ideal $\mathfrak{p}_0 = \mathfrak{J}\cdot(\xi_1 - a_1, \cdots, \xi_n - a_n)$. It is evident that $Q(P)$ is independent of the choice of the non-homogeneous coördinates in $S_n$.

The relationship between the ideal theory of $\mathfrak{J}$ and that of $Q(P) = \mathfrak{J}^*$ is well-known (K, p. 17–20). If $\mathfrak{A}$ is any ideal in $\mathfrak{J}$, its extended ideal $\mathfrak{A}^* = \mathfrak{J}^*\cdot\mathfrak{A}$ in $\mathfrak{J}^*$ is the unit ideal, if $\mathfrak{A} \not\equiv 0(\mathfrak{p}_0)$, and is different from the unit ideal if $\mathfrak{A} \equiv 0(\mathfrak{p}_0)$. Thus all the ideals of $\mathfrak{J}$ which are not multiples of $\mathfrak{p}_0$ are lost in $\mathfrak{J}^*$. In particular, all the zero-dimensional prime ideals of $\mathfrak{J}$, except $\mathfrak{p}_0$, are lost, whence $\mathfrak{J}^*$ *possesses only one prime* 0*-dimensional ideal*, namely $\mathfrak{p}_0^* = \mathfrak{p}_0\cdot\mathfrak{J}^*$. If $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are two ideals in $\mathfrak{J}$, then $\mathfrak{J}^*\cdot\mathfrak{A}_1$ and $\mathfrak{J}^*\cdot\mathfrak{A}_2$ coincide, $\mathfrak{J}^*\mathfrak{A}_1 = \mathfrak{J}^*\mathfrak{A}_2 = \mathfrak{A}^*$, if and only if $\mathfrak{A}_1$ and $\mathfrak{A}_2$ differ by primary components which are not divisible by $\mathfrak{p}_0$. Hence, omitting in $\mathfrak{A}_1$, or in $\mathfrak{A}_2$, all these last mentioned primary components, an ideal $\mathfrak{A}_0$ is obtained which is the h.c.d. of all ideals $\mathfrak{A}$ in $\mathfrak{J}$ such that $\mathfrak{A}^* = \mathfrak{J}^*\mathfrak{A}$. For this ideal $\mathfrak{A}_0$ it can be proved that not only $\mathfrak{A}^* = \mathfrak{J}^*\mathfrak{A}_0$, but that also $\mathfrak{A}_0 = \mathfrak{A}^* \cap \mathfrak{J}$. Thus there is a (1, 1) correspondence (in fact, an isomorphism with respect to all ideal theoretic operations) between the ideals in $\mathfrak{J}^*$ and those ideals in $\mathfrak{J}$ of which every primary component is divisible by $\mathfrak{p}_0$. In this correspondence primary ideals go into primary ideals. In particular, the 1-dimensional ideals $p^*$ in $\mathfrak{J}^*$ correspond to the prime 1-dimensional ideals $\mathfrak{p}$ in $\mathfrak{J}$ which are divisible by $\mathfrak{p}_0$.

Geometrically speaking, the ideal theory of $Q(P) = \mathfrak{J}^*$ is the local ideal theory of the surface $F$ in the neighborhood of the point $P$. Of the irreducible algebraic curves which can be traced on $F$, only those which pass through $P$ are left in the passage from $\mathfrak{J}$ to $Q(P)$.

## 11

We wish to derive some properties of the ideal theory of $Q(P) = \mathfrak{J}^*$ in the case when $P$ is a *simple point* of the surface $F$.

We have shown in $Z_2$ that if $P$ is a simple point, then the corresponding prime 0-dimensional ideal $\mathfrak{p}_0$ does not divide the conductor $\mathfrak{C}$ of $\mathfrak{J}$ with respect to the integral closure $\overline{\mathfrak{J}}$ of $\mathfrak{J}$. We have also shown ($Z_2$, theorem 8) that if $\mathfrak{C} \not\equiv 0(\mathfrak{p}_0)$, then $\mathfrak{p}_0\cdot\overline{\mathfrak{J}} = \bar{\mathfrak{p}}_0$ is a prime (0-dimensional) ideal in $\overline{\mathfrak{J}}$. From these facts it follows that $\mathfrak{J}_{\mathfrak{p}_0} = \mathfrak{J}^* = \overline{\mathfrak{J}}_{\bar{\mathfrak{p}}_0}$. But $\overline{\mathfrak{J}}_{\bar{\mathfrak{p}}_0}$ is integrally closed in $\Sigma$. Hence *the quotient ring* $Q(P)$ *of a simple point is integrally closed in* $\Sigma$.

By our ideal-theoretic definition of a simple point ($Z_2$, section 2), there exists a pair of elements $x, y$ in $\mathfrak{J}$ such that $\mathfrak{p}_0$ is an isolated component of $\mathfrak{J}\cdot(x, y)$. It follows that

$$\mathfrak{p}_0^* = \mathfrak{J}^*\cdot(x, y). \tag{13}$$

Whenever necessary, we shall assume that $x, y$ have been so chosen that the elements of $\mathfrak{J}$ are integrally dependent on $x$ and $y$.

Let $R$ denote the ring of polynomials in $x, y$, $R = \mathsf{K}[x, y]$; let $\mathfrak{P}_0 = R\cdot(x, y)$, and let $R^* = R_{\mathfrak{P}_0}$ be the quotient ring of $\mathfrak{P}_0$ in $R$. We have $R \subset R^* \subseteq \mathfrak{J}^*$,

$R \subseteq \mathfrak{J}$. Ideals in $R$ will be denoted by capital German letters; ideals in $R^*$ will be denoted by capital German letters with an asterisk. Thus $\mathfrak{P}_0^* = \mathfrak{P}_0 \cdot R^*$. We proceed to investigate the *relationship between the ideals in* $\mathfrak{J}^*$ *and those of* $R^*$.

The elements $x$ and $y$ are *uniformizing parameters* of the *complete neighborhood of* $P$ ($Z_2$, section 4). The uniformization is as follows. Given any element $\omega$ in $\mathfrak{J}$, there exists, for any integer $m > 0$, a uniquely determined polynomial $\phi_{m-1}(x, y)$, of degree at most $m - 1$ in $x$ and $y$, such that

$$\omega \equiv \phi_{m-1}(\mathfrak{p}_0^m). \tag{14}$$

Moreover, $\phi_m - \phi_{m-1} = \psi_m$, where $\psi_m$ is a form of degree $m$ in $x$, $y$ (or identically zero). We thus get for $\omega$ a formal power series in $x$, $y$:

$$\omega \to \psi_0 + \psi_1 + \cdots + \psi_m + \cdots, \tag{14'}$$

and (14′) maps $\mathfrak{J}$ isomorphically upon a subring of the ring $\Omega = \mathsf{K}\{x, y\}$ of all formal power series of $x$ and $y$, with coefficients in $\mathsf{K}$.

Here $\psi_0$ is a constant. If $\omega \not\equiv 0(\mathfrak{p}_0)$, then $\psi_0 \neq 0$, since $\omega - \psi_0 \equiv 0(\mathfrak{p}_0)$. Hence the elements of $\mathfrak{J}$ which are not in $\mathfrak{p}_0$ are mapped upon units of $\Omega$. It follows that *the entire quotient ring* $Q(P)$ *is mapped upon a subring of* $\Omega$. We shall see later that *the elements of* $Q(P)$ *are the only elements of the field* $\Sigma$ *which are mapped upon elements of* $\Omega$. Any other element of $\Sigma$ is a *meromorphic* function of $x$ and $y$, i.e. is a quotient of two formal power series, not reducible to a formal power series in $x$ and $y$.

The relation (14) can be expressed symbolically as follows:

$$\mathfrak{J} = (R, \mathfrak{p}_0^m),\ m \text{ arbitrary}, \tag{15}$$

i.e. any element in $\mathfrak{J}$ is the sum of an element in $R$ and of an element in $\mathfrak{p}_0^m$. *We prove a similar relation for* $\mathfrak{J}^*$:

$$\mathfrak{J}^* = (R, \mathfrak{p}_0^{*m}),\ m\text{—an arbitrary integer.} \tag{15'}$$

The proof is immediate. Let $\xi$ be any element in $\mathfrak{J}^*$, and let

$$\xi \to \phi_{m-1} + \psi_m + \psi_{m+1} + \cdots.$$

Then $\xi - \phi_{m-1}$ is represented by the power series $\psi_m + \cdots$ in which the terms of the lowest degree are of degree $\geqq m$. The element $\xi - \phi_{m-1}$ is in $\mathfrak{J}^*$, hence we can write $\xi - \phi_{m-1} = \omega/\omega_0$, where $\omega, \omega_0 \subset \mathfrak{J}$ and $\omega_0 \not\equiv 0(\mathfrak{p}_0)$. Since the power series expansion for $\omega_0$ is a unit in $\Omega$, it follows that the power series for $\omega$ must begin with terms of degree $\geqq m$. Hence, by the nature of our uniformization we must have $\omega \equiv 0(\mathfrak{p}_0^m)$. Consequently $\xi - \phi_{m-1} = \omega/\omega_0 \equiv 0(\mathfrak{p}_0^{*m})$, i.e. $\xi \equiv \phi_{m-1}(\mathfrak{p}_0^{*m})$, where $\phi_{m-1} \subset R$, and this proves (15′). We point out that in the proof just given we have shown incidentally that if the power series expansion for an element $\omega/\omega_0$ in $\mathfrak{J}^*$ begins with terms of degree $\geqq m$, then the element $\omega/\omega_0$ is in $\mathfrak{p}_0^{*m}$. The converse is also true, since $\mathfrak{p}_0^{*m} = \mathfrak{J}^* \cdot (x, y)^m$. Hence $\mathfrak{p}_0^{*m}$ *consists of those and only those elements of* $\mathfrak{J}^*$ *whose power series expansions begin with terms of degree* $\geqq m$.

We have $\mathfrak{p}_0^* = \mathfrak{J}^*\mathfrak{P}_0^*$, where $\mathfrak{P}_0^* = R^* \cdot (x, y)$. Hence also $\mathfrak{p}_0^{*m} = \mathfrak{J}^* \cdot \mathfrak{P}_0^{*m}$. We prove that

$$\mathfrak{P}_0^{*m} = \mathfrak{p}_0^{*m} \cap R^*. \tag{15''}$$

The proof is immediate. Let $g(x, y)/h(x, y)$ be an element of $\mathfrak{p}_0^{*m} \cap R^*$, where $h$ and $g$ are polynomials and $h(0, 0) \neq 0$. The power series for $g/h$ must begin with terms of degree $\geqq m$. Since $h(x, y)$ is a unit, the power series for $g(x, y)$ must begin with terms of degree $\geqq m$. But this power series must be the polynomial $g$ itself, since for all $m$, $0 = g - g \equiv 0(\mathfrak{p}_0^m)$. Hence $g \equiv 0(\mathfrak{P}_0^m)$ and consequently $g/h \equiv 0(\mathfrak{P}_0^{*m})$. Thus $\mathfrak{p}_0^{*m} \cap R^* \subseteq \mathfrak{P}_0^{*m}$. Since $\mathfrak{P}_0^{*m} \subset \mathfrak{p}_0^{*m}$, (15'') follows.

By means of (15') and (15'') we prove the following

THEOREM 1. *There is a* (1,1) *correspondence between the* 0*-dimensional ideals in* $\mathfrak{J}^*$ *and those in* $R^*$. *Two corresponding ideals* $\mathfrak{q}^*$ *and* $\mathfrak{Q}^*$ *are in the relation of extended and contracted ideal respectively*: $\mathfrak{q}^* = \mathfrak{J}^*\mathfrak{Q}^*$, $\mathfrak{Q}^* = \mathfrak{q}^* \cap R^*$.

PROOF. Let $\mathfrak{Q}^* = \mathfrak{q}^* \cap R^*$. To prove that $\mathfrak{q}^* = \mathfrak{J}^*\mathfrak{Q}^*$, it is sufficient to show that $\mathfrak{q}^* \equiv 0(\mathfrak{J}^*\mathfrak{Q}^*)$, since the relation $\mathfrak{J}^*\mathfrak{Q}^* \equiv 0(\mathfrak{q}^*)$ is obviously true. If we choose $m$ sufficiently high so that $\mathfrak{p}_0^{*m} \equiv 0(\mathfrak{q}^*)$ and if we apply (15') to those elements of $\mathfrak{J}^*$ which are in $\mathfrak{q}^*$, we find

$$\mathfrak{q}^* = (R \cap \mathfrak{q}^*, \mathfrak{p}_0^{*m}),$$

hence *a fortiori*:

$$\mathfrak{q}^* = (R^* \cap \mathfrak{q}^*, \mathfrak{p}_0^{*m}), \text{ for all } m \text{ sufficiently high.} \tag{16}$$

The relation (16) holds true for any 0-dimensional ideal in $\mathfrak{J}^*$. We have then $\mathfrak{q}^* = (\mathfrak{Q}^*, \mathfrak{p}_0^{*m})$. Since $\mathfrak{J}^*\mathfrak{Q}^*$ is also zero-dimensional, we can take $m$ sufficiently high so as to have $\mathfrak{p}_0^{*m} = 0(\mathfrak{J}^*\mathfrak{Q}^*)$. Then it will follow that $\mathfrak{q}^* \equiv 0(\mathfrak{Q}^*, \mathfrak{J}^*\mathfrak{Q}^*)$ i.e. $\mathfrak{q}^* \equiv 0(\mathfrak{J}^*\mathfrak{Q}^*)$, q.e.d.

On the other hand, let us start with a 0-dimensional ideal $\mathfrak{Q}^*$ in $R^*$ and let $\mathfrak{J}^*\mathfrak{Q}^* = \mathfrak{q}^*$. To prove that $\mathfrak{q}^* \cap R^* = \mathfrak{Q}^*$, it is sufficient to show that $\mathfrak{q}^* \cap R^* \equiv 0(\mathfrak{Q}^*)$, since $\mathfrak{Q}^* \equiv 0(\mathfrak{q}^*)$. Now, by (15'), we have

$$\mathfrak{q}^* = \mathfrak{J}^*\mathfrak{Q}^* \subseteq (\mathfrak{Q}^*, \mathfrak{p}_0^{*m}),$$

and comparing with (16), we find $(R^* \cap \mathfrak{q}^*, \mathfrak{p}_0^{*m}) \subseteq (\mathfrak{Q}^*, \mathfrak{p}_0^{*m})$, for all $m$ sufficiently high. Consequently

$$R^* \cap \mathfrak{q}^* \subseteq (\mathfrak{Q}^*, \mathfrak{p}_0^{*m}),$$

or

$$R^* \cap \mathfrak{q}^* \subseteq (\mathfrak{Q}^*, \mathfrak{P}_0^{*m}),$$

since, in view of (15''), $\mathfrak{P}_0^{*m}$ is the contracted ideal of $\mathfrak{p}_0^{*m}$. If we now take $m$ sufficiently high so as to have $\mathfrak{P}_0^{*m} \equiv 0(\mathfrak{Q}^*)$, it will follow that $R^* \cap \mathfrak{q}^* \equiv 0(\mathfrak{Q}^*)$, q.e.d.

COROLLARY. *There is also a* (1,1) *correspondence between the zero-dimensional*

*ideals of* $\mathfrak{J}^*$ *and those of the ring* $\Omega$ *of formal power series in* $x$ *and* $y$, *the correspondence being again that of contracted and extended ideal.*

The corollary follows from Theorem 1 and from the well-known fact that a correspondence of the type just mentioned exists between the zero-dimensional ideals of $R^*$ and $\Omega$.[11]

## 12

Let $B_1$ be a zero-dimensional valuation of $\mathsf{K}(x, y)$ whose valuation ring contains $R^*$. The prime ideal of $B_1$ in $R^*$ must be $\mathfrak{p}_0^*$, hence $x$ and $y$ have positive values in $B_1$: $v_{B_1}(x) > 0$, $v_{B_1}(y) > 0$. Similarly let $B$ be a zero-dimensional valuation of $\Sigma$ whose valuation ring contains $\mathfrak{J}^*$. Again (and for a similar reason) we must have $v_B(x) > 0$, $v_B(y) > 0$. The valuation $B$ is said to be an *extended valuation of* $B_1$, *if* $B$ *induces in* $\mathsf{K}(x, y)$ *the valuation* $B_1$. An equivalent condition is the following: the *valuation ring of* $B_1$ *is the intersection of* $\mathsf{K}(x, y)$ *with the valuation ring of* $B$. By general theorems on valuations of algebraic extension fields (van der Waerden [8]) it is well known that if $B_1$ is given, there always exist extended valuations $B$ (always subject to our condition that the valuation rings contain $R^*$ and $\mathfrak{J}^*$ respectively). In the present special case this can also be proved directly in the following fashion. It is well known (and the proof is elementary) that any zero-dimensional valuation $B_1$ of $\mathsf{K}(x, y)$ such that the valuation ring of $B_1$ contains $R^*$, can be extended to a valuation in the field of meromorphic functions of $x$, $y$ whose valuation ring contains $\Omega$. This extended valuation induces a valuation $B$ in $\Sigma$, and $B$ is clearly an extended valuation of $B_1$ of the desired type.

THEOREM 2. *A zero-dimensional valuation* $B_1$ *of* $\mathsf{K}(x, y)$, *whose valuation ring contains* $R^*$, *has a unique extension* $B$ *in* $\Sigma$ *such that the valuation ring of* $B$ *contains* $\mathfrak{J}^*$.

PROOF. Any element $\xi$ in $\Sigma$ can be written in the form $\xi = \omega_1/\omega_2$, where $\omega_1, \omega_2 \subset \mathfrak{J}$. In view of (14) we have: $\omega_1 \equiv \phi_{m-1}^{(1)}(x, y)(\mathfrak{p}_0^m)$, $\omega_2 \equiv \phi_{m-1}^{(2)}(x, y)(\mathfrak{p}_0^m)$. Our proof will consist in showing that if $v_B(\xi) \geqq 0$, then $v_{B_1}(\phi_{m-1}^{(1)}) \geqq v_{B_1}(\phi_{m-1}^{(2)})$, *for all sufficiently high values of* $m$. This will show, namely, that the valuation ring of $B$ is uniquely determined by the valuation ring of $B_1$.

*First case.* $B_1$ *is of rank* 1. If $\mathfrak{A}$ is an ideal (in $R$ or in $\mathfrak{J}$), we denote by $v(\mathfrak{A})$ the minimum value assumed by the elements of $\mathfrak{A}$. Since $v_B(x) > 0$, $v_B(y) > 0$, it follows that $\lim_{m \to +\infty} v(\mathfrak{p}_0^m) = +\infty$. Hence if $m$ is sufficiently large we will have $v_B(\omega_i) = v_{B_1}(\phi_{m-1}^{(i)})$, $i = 1, 2$, and the theorem is proved.

*Second case.* $B_1$ *is of rank* 2. The valuation $B_1$ is composed of a divisor $B_1'$, a one-dimensional valuation. Two cases are possible. Either the prime ideal

[11] This can be proved in exactly the same fashion in which we have proved Theorem 1. Namely, the proof is based entirely on the relations (15′) and (15″). These relations continue to hold (and are trivial) if we replace in them the ring $\mathfrak{J}^*$ by the ring $\Omega$ (and $\mathfrak{p}_0^*$ by the prime ideal $\Omega(x, y)$).

of $B_1'$ in $R$ is the zero-dimensional ideal $\mathfrak{P}_0(B_1'$—a *divisor of second kind with respect to* $R$), or the prime ideal of $B_1'$ in $R$ is a 1-dimensional ideal ($B_1'$—a *divisor of first kind with respect* to $R$). In the first case the divisor $B'$ with which $B$ is composed is also of the second kind with respect to $\mathfrak{J}$ and we will have $v_B(\mathfrak{p}_0) = (m, n)$ where $m > 0$. Hence again $\lim_{m \to +\infty} v(\mathfrak{p}_0^m) = +\infty$, and the remainder of the proof is as in the preceding case of valuations of rank 1. Suppose then that $B_1'$ (and hence also $B'$) is of the first kind with respect to $R$ and $\mathfrak{J}$ respectively. Let $\mathfrak{p}$ be the prime one-dimensional ideal of $B'$ in $\mathfrak{J}$. The element $\xi$ can always be written in the form of a quotient $\omega_1/\omega_2$ where the elements $\omega_1$, $\omega_2$ are not both in $\mathfrak{p}$. If $v_B(\xi) \geqq 0$, then necessarily $\omega_2 \not\equiv 0(\mathfrak{p})$, and the value of $\omega_2$ in $B$ will be of the form $(0, n)$. Hence, if $m$ is sufficiently high, we will have: $v_B(\omega_2) < v_B(\mathfrak{p}_0^m)$, and consequently $v_B(\omega_2) = v_{B_1}(\phi_{m-1}^{(2)}) = (0, n)$. If also $\omega_1 \not\equiv 0(\mathfrak{p})$, then $v_B(\omega_1) = v_{B_1}(\phi_{m-1}^{(1)})$ for all $m$ sufficiently high. If $\omega_1 \equiv 0(\mathfrak{p})$, then $v_B(\omega_1) > v_B(\mathfrak{p}_0^m)$, for all $m$, whence $v_{B_1}(\phi_{m-1}^{(1)}) = v_B(\mathfrak{p}_0^m)$, and consequently $v_{B_1}(\phi_{m-1}^{(1)}) > v_{B_1}(\phi_{m-1}^{(2)})$, for all $m$ sufficiently high. This completes the proof.[12]

## 13

We come now to the one-dimensional ideals in $\mathfrak{J}^*$ and we wish to prove the following theorem:

THEOREM 3. *Every unmixed one-dimensional ideal in* $\mathfrak{J}^*$ *is a principal ideal.*

PROOF. It is sufficient to give the proof for prime ideals. Let $\mathfrak{p}^*$ be a prime one-dimensional ideal in $\mathfrak{J}^*$ and let $\mathfrak{p} = \mathfrak{p}^* \cap \mathfrak{J}$ be the corresponding prime ideal in $\mathfrak{J}$. Also $\mathfrak{p}$ is one-dimensional, and moreover $\mathfrak{p} \equiv 0(\mathfrak{p}_0)$ and $\mathfrak{J}^*\mathfrak{p} = \mathfrak{p}^*$ (see section III, 10). We begin by making a judicious choice of the uniformizing parameters. Any two elements $x_1$ and $y_1$ in $\mathfrak{J}$ can be taken as uniformizing parameters, provided in the expansions $x_1 = ax + by + \cdots$, $y_1 = a'x + b'y + \cdots$, the Jacobian $ab' - a'b$ be different from zero. This, namely, implies that $\mathfrak{p}_0$ is an isolated component of the ideal $\mathfrak{J} \cdot (x', y')$ (see $Z_2$, theorem 1), a characteristic property of uniformizing parameters. Now let $z$ be some element of $\mathfrak{J}$ which is in $\mathfrak{p}_0$ but is not in any of the other possible prime zero-dimensional components of the *zero-dimensional* ideal $\mathfrak{J} \cdot (x, y, \mathfrak{p})$. This implies the relation $\mathfrak{p}_0 = (x, y, z, \mathfrak{p})$. We put $x_1 = c_1x + c_2y + c_3z$, $y_1 = c_1'x + c_2'y + c_3'z$. We choose "non-special" values for the coefficients $c$ and $c'$, so as to satisfy the following three conditions: (1) $x_1$, $y_1$ are uniformizing parameters; (2) the elements of $\mathfrak{J}$ (which, by our initial choice of $x$ and $y$, are integrally dependent on $x$, $y$) are integrally dependent on $x_1$, $y_1$; (3) $\mathfrak{J} \cdot (x_1, y_1, \mathfrak{p}) = \mathfrak{p}_0$.

That conditions (1) and (2) can be satisfied is trivial. As for (3) we observe that if $c_1$, $c_2$, $c_3$ are non-special constants, then the ideal $\mathfrak{J} \cdot (x_1, \mathfrak{p})$ is zero-dimensional. In view of our choice of $z$, it is clear that of the prime ideals of $\mathfrak{J} \cdot (x_1, \mathfrak{p})$, only $\mathfrak{p}_0$ contains all the three elements $x$, $y$ and $z$. Hence, if $c_1'$,

[12] A few additional considerations would make it quite clear that the preceding proof contains implicitly the proof of *existence* of an extended valuation $B$.

$c_2', c_3'$ are non-special constants, also $y_1$ will belong to $\mathfrak{p}_0$ but not to any of the remaining prime ideals of $\mathfrak{J}\cdot(x_1, \mathfrak{p})$. If in addition $x_1$, $y_1$ are uniformizing parameters, $\mathfrak{p}_0$ will be an isolated component of $\mathfrak{J}\cdot(x_1, y_1)$, whence $\mathfrak{p}_0 = \mathfrak{J}\cdot(x_1, y_1, \mathfrak{p})$.

We shall assume that our original uniformizing parameters $x$ and $y$ already satisfy the above three conditions, in particular:

$$\mathfrak{p}_0 = \mathfrak{J}\cdot(x, y, \mathfrak{p}). \tag{17}$$

Let $\omega_1, \cdots, \omega_m$ be elements of $\mathfrak{J}$ which form a base for $\mathfrak{p}$. Let $\mathfrak{p}_0^{(1)}, \cdots, \mathfrak{p}_0^{(h)}$ be the prime ideals belonging to the ideal $\mathfrak{J}\cdot(x, y)$ and different from $\mathfrak{p}_0$. In view of (17) it is clear that for non-special coefficients $c_i$ the element $c_1\omega_1 + \cdots + c_m\omega_m$ will not belong to any of the ideals $\mathfrak{p}_0^{(j)}$, $j = 1, 2, \cdots, h$. Hence, applying if necessary a preliminary linear homogeneous transformation to the elements $\omega_i$, we may assume that $\omega_i \not\equiv 0(\mathfrak{p}_0^{(j)})$, $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, h$. By Theorem 4 of $Z_2$ we have the following: let $F_i(x, y, t) = N(t - \omega_i)$ = norm of $t - \omega_i$ with respect to the field $\mathsf{K}(x, y)$; *then* $t = 0$ *is a simple root of* $F_i(0, 0, t)$. We can write then $F_i$ in the form $F_i = t\cdot H_i(x, y, t) - A_i(x, y)$, where $H_i(0, 0, 0) \neq 0$ and $A_i$ is a polynomial. Since $F_i(x, y, \omega_i) = 0$, it follows that $\omega_i\cdot H_i(x, y, \omega_i) = A_i(x, y)$, where $H_i(x, y, \omega_i) \not\equiv 0(\mathfrak{p}_0)$ (since $x$, $y$ and $\omega_i$ are all $\equiv 0 \pmod{\mathfrak{p}_0}$). Now let $g = g(x, y)$ be the *irreducible* polynomial in $x$, $y$ which belongs to $\mathfrak{p}$; in other words: let $\mathfrak{p} \cap R$ be the principal prime ideal $R.g$. Since $\omega_i \equiv 0(\mathfrak{p})$, also $A_i \equiv 0(\mathfrak{p})$, and since $A_i \subset \mathsf{K}[x, y]$, $A_i$ must be divisible by $g$. Since $H_i(x, y, \omega_i) \not\equiv 0(\mathfrak{p}_0)$, we conclude that

$$\omega_i \equiv 0(\mathfrak{J}^*g), \qquad i = 1, 2, \cdots, m,$$

or, since $\mathfrak{p}^* = \mathfrak{J}^*\mathfrak{p} = \mathfrak{J}^*(\omega_1, \cdots, \omega_m)$,

$$\mathfrak{p}^* \equiv 0(\mathfrak{J}^*g).$$

Since, on the other hand, $g \equiv 0(\mathfrak{p}) \equiv 0(\mathfrak{p}^*)$, we conclude with the relation $\mathfrak{p}^* = \mathfrak{J}^*g$, and this proves our theorem.

COROLLARY. $\mathfrak{J}^*$ *coincides with the totality of elements of the field* $\Sigma$ *which are mapped upon formal power series in* $x$ *and* $y$. We have to show that if $\alpha$, $\beta$ are two elements in $\mathfrak{J}^*$ and if $\alpha$ is divisible by $\beta$ in $\mathsf{K}\{x, y\}(= \Omega)$, *then* $\alpha$ *is also divisible by* $\beta$ *in* $\mathfrak{J}^*$. The element $\alpha$ belongs to the principal ideal $\Omega\beta$. This ideal is one-dimensional and unmixed in $\Omega$. Hence its contracted ideal in $\mathfrak{J}^*$ is also one-dimensional and unmixed.[13] By the preceding theorem we can write: $\Omega\beta \cap \mathfrak{J}^* = \mathfrak{J}^*\beta'$, $\beta' \subset \mathfrak{J}^*$, whence $\alpha$ is divisible by $\beta'$ in $\mathfrak{J}^*$. It remains to prove that $\beta'$ is divisible by $\beta$ in $\mathfrak{J}^*$. We have $\beta = \epsilon\beta'$, where $\epsilon \subset \mathfrak{J}^*$. On the other hand $\beta'$ is in $\Omega\beta$, i.e. $\beta'$ is at any rate divisible by $\beta$ in $\Omega$. *Hence* $\epsilon$ *is necessarily a unit in* $\Omega$. Now the elements of $\mathfrak{J}^*$ which are mapped upon units

[13] If $\bar{\mathfrak{p}} = \Omega\cdot\xi$ is a prime 1-dimensional ideal in $\Omega$ ($\xi$—a prime element in $\Omega$, not a unit), the contracted ideal of $\bar{\mathfrak{p}}$ in $\mathfrak{J}^*$ may be the zero-ideal, but clearly is never the zero-dimensional ideal $\mathfrak{p}_0^* = \mathfrak{J}^*(x, y)$. Since $\beta$ is in $\mathfrak{J}^*$, the contracted ideal of $\Omega\beta$ is not the zero-ideal.

of $\Omega$ are those and only those which are not in $\mathfrak{p}_0^*$. Consequently $\epsilon \not\equiv 0(\mathfrak{p}_0^*)$, and hence $\frac{1}{\epsilon}$ is also an element of $\mathfrak{J}^*$. Since $\beta' = \frac{1}{\epsilon} \cdot \beta$, the corollary follows.

## IV. Quotient Rings on Normal Surfaces

### 14

After having fully discussed in Part III the properties of the quotient ring of a simple point, we now wish to discuss more generally the structure of the quotient ring $Q(P)$ of a point $P$ of a *normal surface* $F$. The hypothesis that $F$ is normal implies that $Q(P)$ is integrally closed in $\Sigma$. It is this last local property which matters, rather than the property at large to the effect that $F$ is normal. Namely, were $F$ not normal and $P$ a point of $F$ such that $Q(P)$ is integrally closed in $\Sigma$, then we can always replace $F$ by any of the normal surfaces $F^*$ determined by $F$. To $P$ there corresponds a unique point $P^*$ of $F^*$, and the quotient ring of $P^*$ coincides with $Q(P)$. It is therefore to us only a matter of convenience, when, in studying the structure of an integrally closed quotient ring $Q(P)$, we think of $P$ as a point of a normal surface.

The class of integrally closed quotient rings $Q(P)$ whose structure we seek to determine will be, however, somewhat special. *We shall assume namely that $Q(P)$ contains as a subring the quotient ring $Q(A)$ of a simple point $A$.* For the applications which we wish to make in the sequel, the consideration of such special quotient rings is sufficient. On the other hand, we may observe that the condition imposed by us on $Q(P)$ is consistent with highly complicated types of singular points $P$.

Our study of the structure of $Q(P)$ will be based upon the results of the preceding section, as applied to the quotient ring of the simple point $A$, and also on the theory of valuation ideals in a ring $\mathsf{K}\{x, y\}$ of formal power series of two variables, developed in $Z_1$. In view of the isomorphism between the zero-dimensional ideals in $Q(A)$ and in $\mathsf{K}\{x, y\}$ ($x, y$—uniformizing parameters at $A$), the results of that paper are directly applicable to $Q(A)$.

First we shall need a few clear-cut definitions and statements concerning the correspondence between the points of two birationally equivalent surfaces. In agreement with our point of view, we base our definitions on valuation theory.

Let $F$ and $F'$ be birationally equivalent surfaces, projective models of the field $\Sigma$. The coördinates $\xi_1', \cdots, \xi_m'$ of the general point of $F'$ are rational functions of the coördinates $\xi_1, \cdots, \xi_n$ of the general point of $F$, and *vice versa*. The birational transformation from $F$ to $F'$ sets up a *correspondence between the points of the surfaces.* For our present purpose, the most convenient definition of this correspondence is the following: *a point $P$ on $F$ and a point $P'$ on $F'$ correspond to each other, if there exists a zero-dimensional valuation $B$ of the field $\Sigma$, such that $P$ is the center of $B$ on $F$ and $P'$ is the center of $B$ on $F'$.*[14] *A point $P$*

[14] In other words: there exists a branch on $F$, with origin at $P$, to which there corresponds a branch on $F'$, with origin at $P'$.

*on $F$ is a fundamental point,* if there exist a 1-dimensional valuation $B_1$ of $\Sigma$, such that the center of $B_1$ on $F$ is the point $P$, while the center of $B_1$ on $F'$ is a curve $\Gamma$ (necessarily irreducible).[15] The curve $\Gamma$ is a *fundamental curve* and is said to correspond to the point $P$. Every point $P'$ of $F'$ which is on the curve $\Gamma$ corresponds to at least one place of the field of rational functions on $\Gamma$. Such a place defines a zero-dimensional valuation of $\Sigma$ (composed with the divisor $B_1$) whose center on $F'$ is $P'$ and whose center on $F$ is $P$. Hence $P$ *corresponds to any point of the fundamental curve* $\Gamma$.

It is clear that if $P$ is the center of a zero-dimensional valuation $B$, then the valuation ring of $B$ contains the quotient ring $Q(P)$, and conversely. It follows that *if $P$ and $P'$ are two corresponding points of $F$ and $F'$ respectively and if $Q(P') \subseteq Q(P)$, then $P'$ is the only point of $F'$ which corresponds to $P$,* and thus $P$ is not a fundamental point.

THEOREM 4. *The locus of points $P'$ which correspond to a given point $P$ of $F$ is an algebraic variety of dimension $\leqq 1$. Every one-dimensional irreducible component of this variety is a fundamental curve corresponding to $P$.*

PROOF. It will be sufficient to prove this theorem for the points at finite distance of $F$ and $F'$, since we can choose for either surface the hyperplane at infinity arbitrarily.

We denote the rings $\mathsf{K}[\xi_1, \cdots, \xi_n]$ and $\mathsf{K}[\xi_1', \cdots, \xi_m']$ by $\mathfrak{J}$ and $\mathfrak{J}'$ respectively, and we consider the join $\bar{\mathfrak{J}} = (\mathfrak{J}, \mathfrak{J}') = \mathsf{K}[\xi; \xi']$ of the two rings (the smallest ring containing both $\mathfrak{J}$ and $\mathfrak{J}'$). The ring $\bar{\mathfrak{J}}$ defines an algebraic surface $\bar{F}$ in an affine space $S_{n+m}$. The coördinates of the general point of $F_1$ are $\xi_1, \cdots, \xi_n, \xi_1', \cdots, \xi_m'$ and $\bar{F}$ is birationally equivalent to $F$ and $F'$. If $\bar{P}$ is any point at finite distance on $\bar{F}$, it is given by a prime zero-dimensional ideal $\bar{\mathfrak{p}}_0$ in $\bar{\mathfrak{J}}$. The contracted ideals $\mathfrak{p}_0 = \mathfrak{J} \cap \bar{\mathfrak{p}}_0$, $\mathfrak{p}_0' = \mathfrak{J}' \cap \bar{\mathfrak{p}}_0$ are prime and zero-dimensional and define a point $P$ and a point $P'$ on $F$ and $F'$ respectively. It is clear that $Q(\bar{P}) \supseteqq Q(P)$, $Q(\bar{P}) \supseteqq Q(P')$. Hence any zero-dimensional valuation of center $\bar{P}$ has $P$ as its center on $F$ and $P'$ as its center on $F'$. Consequently, *to a point $\bar{P}$ on $\bar{F}$ (at finite distance) there corresponds a unique point $P$ on $F$ and a unique point $P'$ on $F'$, and $P$, $P'$ are corresponding points.* Conversely, let $P$ and $P'$ be two corresponding points (at finite distance) of $F$ and $F'$ respectively. There exists then a zero-dimensional valuation $B$ whose center on $F$ is $P$ and whose center on $F'$ is $P'$. Since the valuation ring of $B$ contains both rings $\mathfrak{J}$ and $\mathfrak{J}'$, it also contains their join $\bar{\mathfrak{J}}$. Hence the center of $B$ on $\bar{F}$ is at a point $\bar{P}$ at finite distance. The points $P$, $P'$, $\bar{P}$ being the centers of the valuation $B$ on $F$, $F'$, $\bar{F}$ respectively, the points, $P$, $P'$, must be *the points* which correspond to the point $\bar{P}$. We conclude with the following:

[15] We speak of the center of a 1-dimensional valuation in the following sense. Given $B_1$, we can so choose the non-homogeneous coördinates $\xi_i$ that their values in $B_1$ be non-negative. Then the valuation ring of $B_1$ contains the ring $\mathsf{K}[\xi_1, \cdots, \xi_m]$. The prime ideal of $B_1$ in this ring is either zero-dimensional or one-dimensional. In the first case the center of $B_1$ on $F$ is a point and $B_1$ is a divisor of the second kind (with respect to the ring $\mathsf{K}[\xi]$). In the second case *the center of* $B_1$ is an irreducible curve on $F$, and $B_1$ is a divisor of the first kind.

*The points $\tilde{P}$ at finite distance of $\tilde{F}$ are in* (1, 1) *correspondence, without exceptions, with the pairs* $(P, P')$ *of corresponding points of* $F$ *and* $F'$ (at finite distance).

Let $P$ be an arbitrary point at finite distance on $F$, $\mathfrak{p}_0$—its prime zero-dimensional ideal in $\mathfrak{J}$. Let $\tilde{\mathfrak{J}} \cdot \mathfrak{p}_0 = \tilde{\mathfrak{A}}$ and let $[\tilde{\mathfrak{A}}, \mathfrak{J}'] = \mathfrak{A}'$. We assert that *the algebraic locus* $\Gamma'$ *determined on* $F'$ *by the ideal* $\mathfrak{A}'$ *is the locus of points at finite distance which correspond to* $P$. In fact, let $P'$ be a point of $F'$, at finite distance, which corresponds to $P$, and let $\mathfrak{p}_0'$ be the prime zero-dimensional ideal in $\mathfrak{J}'$ given by the point $P'$. Let, moreover, $\tilde{P}$ be the point on $\tilde{F}$ which corresponds to the point-pair $(P, P')$, and let $\tilde{\mathfrak{p}}_0$ be the corresponding prime zero-dimensional ideal in $\tilde{\mathfrak{J}}$. Since $\tilde{P} \to P$, we must have $\mathfrak{p}_0 = \tilde{\mathfrak{p}}_0 \cap \mathfrak{J}$, whence $\tilde{\mathfrak{J}} \cdot \mathfrak{p}_0 \equiv 0(\tilde{\mathfrak{p}}_0)$, i.e. $\tilde{\mathfrak{A}} \equiv 0(\tilde{\mathfrak{p}}_0)$. Since $\tilde{P} \to P'$ we also have $\mathfrak{p}_0' = \tilde{\mathfrak{p}}_0 \cap \mathfrak{J}$, hence $\mathfrak{A}' \equiv 0(\mathfrak{p}_0')$. This proves that $P'$ is on $\Gamma'$.

Consider now the irreducible components of $\Gamma'$. They may be points or curves and they are given by the isolated prime ideals of $\mathfrak{A}'$. Since $\mathfrak{A}' = [\tilde{\mathfrak{A}}, \mathfrak{J}']$, it is clear that each isolated prime ideal $\mathfrak{p}'$ of $\mathfrak{A}'$ is the contracted ideal of some prime ideal $\tilde{\mathfrak{p}}$ of $\tilde{\mathfrak{A}}$. Moreover, since $\mathfrak{p}_0 \subseteq \tilde{\mathfrak{A}}$, also $\mathfrak{p}_0 \subseteq \tilde{\mathfrak{p}}$, whence $\tilde{\mathfrak{p}} \cap \mathfrak{J} = \mathfrak{p}_0$ and $\tilde{\mathfrak{p}} \cap \mathfrak{J}' = \mathfrak{p}'$. There always exists a valuation whose center on $\tilde{F}$ is $\tilde{\mathfrak{p}}$ (i.e. the corresponding point or curve, according as $\tilde{\mathfrak{p}}$ is zero-dimensional or one-dimensional). The center of this valuation on $F$ is $P$ and its center on $F'$ is the irreducible component of $\Gamma'$ given by the ideal $\mathfrak{p}'$. Hence every irreducible component of $\Gamma'$ corresponds to $P$, and this completes the proof of theorem 4.

A consequence of Theorem 4, which we shall have occasion to use in the sequel, is the following

THEOREM 5. *If* $Q(P)$ *is integrally closed in* $\Sigma$ *and if* $P$ *is not a fundamental point, then to* $P$ *there corresponds a unique point* $P'$ *on* $F'$.

PROOF. By Theorem 4, our hypothesis that $P$ is not fundamental implies at any rate that to $P$ there corresponds on $F'$ only a finite number of points, say $P_1', P_2', \cdots P_\sigma'$. We may assume these points to be at finite distance. Let $\mathfrak{p}_0^{(1)}, \mathfrak{p}_0^{(2)}, \cdots, \mathfrak{p}_0^{(\sigma)}$ be the corresponding prime zero-dimensional ideals in $\mathfrak{J}'$. We denote by $\Delta$ *the intersection of the quotient rings* $Q(P_1'), Q(P_2'), \cdots, Q(P_\sigma')$. If $B$ is any zero-dimensional valuation whose center is $P$, its center on $F'$ will be one of the points $P_1', \cdots, P_\sigma'$. Hence the valuation ring of $B$ will contain one of the quotient rings $Q(P_1'), \cdots, Q(P_\sigma')$, and hence it will certainly contain $\Delta$. Hence, if *the valuation ring of a zero-dimensional valuation* $B$ *contains* $Q(P)$, *it also contains* $\Delta$. Since $Q(P)$ is integrally closed, it is the intersection of all the valuation rings which contain it (K, p. 111), and, moreover, it is not difficult to see that in the representation of $Q(P)$ as an intersection of valuation rings it is permissible to omit the one-dimensional valuations.[16] We conclude

[16] A one-dimensional valuation $B_1$ defines an homomorphic mapping of the valuation ring $\mathfrak{B}_1$ of $B_1$ upon a field $\Sigma^*$ of algebraic functions of one variable. If $Q(P)$ is contained in $\mathfrak{B}_1$, then $\mathfrak{J}$ is mapped upon a finite integral domain $\mathfrak{J}^*$ contained in $\Sigma^*$, and $Q(P)$ is mapped upon the quotient ring $Q(P^*)$ of a prime ideal in $\mathfrak{J}^*$. The ring $Q(P^*)$ is contained in at least one valuation ring (defined by a "place" of the field $\Sigma^*$). Hence $Q(P)$ is contained in the valuation ring $\mathfrak{B}$ of the corresponding zero-dimensional valuation $B$ of $\Sigma$. Since $\mathfrak{B} \subset \mathfrak{B}_1$, our assertion follows.

that $\Delta$ *is contained in* $Q(P)$. Let $\mathfrak{p}_i'$ be the zero-dimensional prime ideal of $Q(P_i')$, $i = 1, 2, \cdots, \sigma$, and let $\mathfrak{p}_i^* = \Delta \cap \mathfrak{p}_i'$. Let us assume that $\sigma > 1$. The $\sigma$ prime ideals $\mathfrak{p}_1^*, \cdots, \mathfrak{p}_\sigma^*$ in $\Delta$ are distinct, since we can always find an element of $\Delta$ which is in $\mathfrak{p}_i^*$ and not in $\mathfrak{p}_j^*$, if $i \neq j$ (such an element already exists in $\mathfrak{F}'$). Let $\xi'$ be an element of $\mathfrak{p}_1^*$, not in $\mathfrak{p}_2^*$. There exists a valuation $B_1$ whose center on $F$ is at $P$ and whose center on $F'$ is $P_1'$. Since $\xi'$ belongs to the prime ideal of $Q(P_1')$, necessarily $v_{B_1}(\xi') > 0$. Hence $\xi'$ belongs to the prime zero-dimensional ideal of $Q(P)$. But then necessarily $\xi'$ has a positive value in any valuation whose center is the point $P$. In particular, let $B_2$ be a zero-dimensional valuation whose center on $F$ is $P$ and whose center on $F'$ is $P_2'$. Since $v_{B_2}(\xi') > 0$, $\xi'$ must belong to the prime ideal $\mathfrak{p}_2'$ of $Q(P_2')$. Hence $\xi' \subset \mathfrak{p}_2^*$, a contradiction.

Consequently $\sigma = 1$, q.e.d.

## 15

After these preliminaries, we come back to the question announced at the beginning of the preceding section. We consider a surface $F$, given in the affine space by a ring $\mathfrak{F} = \mathsf{K}[\xi_1, \cdots, \xi_n]$, and on $F$ we consider a point $P$ such that $Q(P)$ is integrally closed in $\Sigma$. We assume that $P$ is a point at finite distance, so that $P$ is given by a prime zero-dimensional ideal in $\mathfrak{F}$, say by the ideal $\mathfrak{F} \cdot (\xi_1, \cdots, \xi_n)$. As was pointed out before, we may assume, without loss of generality, that $\mathfrak{F}$ itself is integrally closed.

We assume that $Q(P)$ contains the quotient ring $Q(A)$ of a *simple* point $A$ of another surface $\Phi$, birationally equivalent to $F$. We know that $Q(A)$ is integrally closed in $\Sigma$. Let $\Phi$ be given in an affine space $S_m$ by the ring $\mathfrak{o} = \mathsf{K}[\omega_1, \cdots, \omega_m]$. As in the preceding case of $F$ and $P$, we assume also here that $A$ is a point at finite distance, that it is given in $\mathfrak{o}$ by the prime ideal $\mathfrak{o} \cdot (\omega_1, \cdots, \omega_m)$ and that $\mathfrak{o}$ is integrally closed in $\Sigma$.

The fact that $Q(P)$ contains $Q(A)$ does not necessarily imply that $\mathfrak{F}$ contains $\mathfrak{o}$. However, we may replace $\mathfrak{F}$ by the join $\mathfrak{F}_1 = (\mathfrak{F}, \mathfrak{o})$. The point pair $(P, A)$ is represented by a prime zero-dimensional ideal $\mathfrak{p}_0^{(1)}$ in $\mathfrak{F}_1$, and since $Q(P) \supseteq Q(A)$, it is immediately seen that $Q(P)$ coincides with the quotient ring of $\mathfrak{p}_0^{(1)}$ in $\mathfrak{F}_1$. Hence we may replace $P$ by the corresponding point $P_1$ on the surface defined by $\mathfrak{F}_1$ in the affine space. If $\mathfrak{F}_1$ is not integrally closed, we replace $\mathfrak{F}_1$ by its integral closure. *We assume then that* $\mathfrak{F} \supseteq \mathfrak{o}$. Under this assumption we have $\mathsf{K}[\xi_1, \cdots, \xi_n] = \mathsf{K}[\xi_1, \cdots, \xi_n, \omega_1, \cdots, \omega_m]$. We may then include the $\omega$'s among the generators of $\mathfrak{F}$, and therefore it is permissible to assume that

$$\xi_i = \omega_i, \qquad i = 1, 2, \cdots, m; \; n \geqq m. \tag{18}$$

We shall denote by $\mathfrak{F}^*$ and $\mathfrak{o}^*$ the quotient rings $Q(P)$ and $Q(A)$ respectively. Their prime zero-dimensional ideals shall be denoted by $\mathfrak{P}_0$ and $\mathfrak{p}_0$ respectively. Let

$$\xi_i = \frac{\phi_i(\omega_1, \cdots, \omega_m)}{\phi_0(\omega_1, \cdots, \omega_m)}, \qquad i = 1, 2, \cdots, n, \tag{19}$$

where the $\phi$'s are polynomials, and

$$\phi_i = \omega_i \phi_0 , \qquad i = 1, 2, \cdots , m, \tag{19'}$$

in view of (18). We consider the following ideals in $\mathfrak{o}^*$

$$\mathfrak{M} = \mathfrak{o}^* \cdot (\phi_0 , \phi_1 , \cdots , \phi_n),$$
$$\mathfrak{m} = \mathfrak{o}^* \cdot (\phi_1 , \cdots , \phi_n). \tag{20}$$

*We may assume that* $\mathfrak{M}$ *and* $\mathfrak{m}$ *are zero-dimensional.* In fact, if $\mathfrak{M}$ is one-dimensional, then by theorem 3 (II) we can write

$$\epsilon \phi_i = g(\omega_1 , \cdots , \omega_m)\psi_i(\omega_1 , \cdots , \omega_m), \qquad i = 0, 1, \cdots , n,$$

where $\epsilon$ is a unit in $\mathfrak{o}^*$, $g$ and $\psi_i$ are polynomials and $\psi_0 , \cdots , \psi_n$ have no common factor in $\mathfrak{o}^*$ (not a unit). We then replace $\phi_0 , \cdots , \phi_n$ by $\psi_0 , \cdots , \psi_n$ respectively, since $\xi_i = \psi_i/\psi_0$, and then $\mathfrak{M}$ will be zero-dimensional.[17]

By (19'), a common factor of $\phi_1 , \cdots , \phi_n$ (in $\mathfrak{o}^*$) has to divide $\phi_0$. Hence if $\mathfrak{M}$ is already zero-dimensional, also $\mathfrak{m}$ is zero-dimensional.

We denote by $M$ the totality of all zero-dimensional valuations $B$ of $\Sigma$ such that the center of $B$ on $F$ is the point $P$, or, in other words, such that the valuation ring $\mathfrak{B}$ of $B$ contains $Q(P)$. Consider any member $B$ of $M$. Since $Q(P) \supset Q(A)$, we have $\mathfrak{B} \supset Q(A)$, and we are in position to consider the *v-ideals* (*valuation ideals*) in $Q(A)$ belonging to the valuation $B$ (see $Z_1$). Let $\mathfrak{q}$ be the $v$-ideal such that $v(\mathfrak{q}) = v(\phi_0)$. We consider *the intersection* of all these $v$-ideals $\mathfrak{q}$ as $B$ varies in $M$. We denote this intersection by $\mathfrak{A}$. In the terminology of our paper $Z_1$, $\mathfrak{A}$ is a *complete ideal.*

Again for a fixed $B$ in $M$, we consider the $v$-ideal $\mathfrak{q}_1$ in $\mathfrak{o}^*$ which follows immediately the above $v$-ideal $\mathfrak{q}$, i.e. the first $v$-ideal $\mathfrak{q}_1$ such that $v(\mathfrak{q}_1) > v(\mathfrak{q})$. We denote by $\mathfrak{a}$ the intersection of all ideals $\mathfrak{q}_1$, as $B$ varies in $M$. Also $\mathfrak{a}$ is a complete ideal.

Since $\mathfrak{J}^* \cdot (\xi_1 , \cdots , \xi_n) = \mathfrak{P}_0$, it follows that $v_B(\xi_i) > 0$, for any $B$ in $M$ and for $i = 1, 2, \cdots , n$. Hence $v_B(\phi_i) > v_B(\phi_0)$, $i \neq 0$, and consequently $\phi_i \subset \mathfrak{q}$, $i = 0, 1, \cdots , n$, and $\phi_i \subset \mathfrak{q}_1$, $i = 1, 2, \cdots , n$. *We conclude that* $\mathfrak{M} \subseteq \mathfrak{A}$, $\mathfrak{m} \subseteq \mathfrak{a}$ *and that*

$$v_B(\mathfrak{A}) = v_B(\phi_0) > 0, \tag{21}$$

$$v_B(\mathfrak{a}) > v_B(\phi_0) > 0, \tag{21'}$$

for any $B$ in $M$. Since $v_B(\phi_0) > 0$ ($\phi_0$ is not a unit in $\mathfrak{o}^*$, see footnote 17), $\mathfrak{A}$ is not the unit ideal. Since $\mathfrak{M}$ and $\mathfrak{m}$ are *zero-dimensional,* it follows that *both* $\mathfrak{A}$ *and* $\mathfrak{a}$ *are zero-dimensional complete ideals.*

[17] Strictly speaking, it may happen that after this reduction $\mathfrak{M}$ is the unit ideal. Since $\xi_1 , \cdots , \xi_n$ are in the prime ideal $\mathfrak{P}_0$ of $\mathfrak{o}^*$ and since $\xi_i \phi_0 = \phi_i$, it follows that $\phi_i \equiv 0(\mathfrak{p}_0)$, $i = 1, \cdots , n$. Hence necessarily $\phi_0$ must be a unit in $\mathfrak{o}^*$, and therefore each $\xi_i$ is in $\sigma^*$. That implies that $Q(P)$ coincides with $Q(A)$. We naturally exclude this trivial case.

THEOREM 6. *The ideal* $\mathfrak{a}$ *is a maximal subideal of* $\mathfrak{A}$. *The ring of residual classes* $\mathfrak{A}/\mathfrak{a}$ *is a* $\mathsf{K}$*-module of rank* 1.

PROOF. Let $\alpha$ be any element in $\mathfrak{A}$. By (21), we have $v_B(\alpha/\phi_0) \geqq 0$ for any $B$ in $M$. Since $Q(P)$ is integrally closed, it is the intersection of the valuation rings $\mathfrak{B}$, as $B$ varies in $M$ (see footnote 16). Hence $\alpha/\phi_0$ is an element of $Q(P)$. There exists then a constant $c$ in $\mathsf{K}$ such that $\alpha/\phi_0 \equiv c(\mathfrak{P}_0)$. For such a constant $c$ it is then true that $v_B(\alpha - c\phi_0) > v_B(\phi_0)$, for all $B$ in $M$. Hence $\alpha - c\phi_0$ is an element of the $v$-ideal $\mathfrak{q}_1$, for any $B$ in $M$, i.e. $\alpha - c\phi_0 \equiv 0(\mathfrak{a})$. This shows that $\mathfrak{A}/\mathfrak{a}$ is a $\mathsf{K}$-module of rank 1 (having $\phi_0$ as base) and that consequently $\mathfrak{a}$ is a maximal subideal of $\mathfrak{A}$, q.e.d.

In the course of this proof we have shown that if $\alpha$ is any element in $\mathfrak{A}$, then $\alpha/\phi_0$ is an element of $Q(P)$. Notice that $\phi_0$ is an element of $\mathfrak{A}$, but not of $\mathfrak{a}$ (in view of (21′)). Now, more generally, we can prove the following

THEOREM 7. *If* $\alpha, \beta \subset \mathfrak{A}$, $\beta \not\subset \mathfrak{a}$, *then* $\alpha/\beta \subset Q(P)$; *moreover* $\alpha/\beta \subset \mathfrak{P}_0$, *if and only if* $\alpha \subset \mathfrak{a}$.

PROOF. Since $\beta \not\subset \mathfrak{a}$, there exists a valuation $B$ in $M$ such that $\beta \not\subset \mathfrak{q}_1$, since $\mathfrak{a}$ is the intersection of the $v$-ideals $\mathfrak{q}_1$. Since $\mathfrak{q}_1$ is the immediate successor of $\mathfrak{q}$, it follows that $v_B(\beta) = v_B(\mathfrak{q}) = v_B(\phi_0)$. This implies that $\beta/\phi_0$, which we know already to be an element of $Q(P)$, is *not in the prime ideal* $\mathfrak{P}_0$ of $Q(P)$. Therefore we must have $v_B(\beta) = v_B(\phi_0)$, *for any valuation* $B$ in $M$. Consequently, $v_B(\alpha/\beta) \geqq 0$ for any $B$ in $M$, and this implies $\alpha/\beta \subset Q(P)$.

The second part of the theorem is now a straightforward consequence of the fact that $\alpha/\beta$ is an element of $\mathfrak{P}_0$, if and only if $v_B(\alpha/\beta) > 0$, $B \subset M$.

Theorem 7 gives the quotient representation only for *certain* elements of $\mathfrak{Z}^*$, because naturally, if $\alpha/\beta$ is a quotient of the indicated form, then $\alpha^\rho/\beta^\rho$, $\rho$—an integer, will not, in general, be representable as a quotient of two elements $\alpha', \beta'$ of $\mathfrak{A}$ such that $\beta'$ is not $\mathfrak{a}$. The main result of the present considerations is the following theorem, which gives full information concerning the connection between the complete ideals $\mathfrak{A}$, $\mathfrak{a}$, and the representation of any element in $\mathfrak{Z}^*$ as a quotient of elements in $\mathfrak{o}^*$:

THEOREM 8. *If* $\rho$ *is an integer* $> 0$ *and* $\alpha, \beta$ *are two elements in* $\mathfrak{o}^*$ *such that* $\alpha, \beta \equiv 0(\mathfrak{A}^\rho)$, $\beta \not\equiv 0(\mathfrak{A}^{\rho-1}\mathfrak{a})$, *then* $\alpha/\beta$ *is an element of* $\mathfrak{Z}^*$, *and in this fashion all the elements of* $\mathfrak{Z}^*$ *can be obtained.* The above element $\alpha/\beta$ *is in the prime zero-dimensional ideal* $\mathfrak{P}_0$ *of* $\mathfrak{Z}^*$, *if and only* if $\alpha \equiv 0(\mathfrak{A}^{\rho-1}\mathfrak{a})$.

PROOF. The products $\omega_1\phi_0, \cdots, \omega_m\phi_0$ have values greater than $v(\phi_0)$ in any valuation $B$ in $M$, hence they are elements of $\mathfrak{a}$ (this also follows directly from theorem 6). Therefore, by Theorem 6, any element $\gamma$ of $\mathfrak{A}^\rho$ can be written in the form $c\phi_0^\rho + \gamma_1$, where $c$ is a constant and $\gamma \subset \mathfrak{A}^{\rho-1}\mathfrak{a}$. Since $v_B(\mathfrak{A}^{\rho-1}\mathfrak{a}) > \rho v_B(\phi_0)$, for any $B$ in $M$, it follows that $\mathfrak{A}^{\rho-1}\mathfrak{a}$ *is a proper maximal subideal* of $\mathfrak{A}^\rho$. Now let $\alpha, \beta$ be two elements of $\mathfrak{o}^*$ such that $\alpha, \beta \equiv 0(\mathfrak{A}^\rho)$, $\beta \not\equiv 0(\mathfrak{A}^{\rho-1}\mathfrak{a})$. Then we can write $\alpha = c\phi_0^\rho + \alpha_1, \beta = d\phi_0^\rho + \beta_1$, where $\alpha_1, \beta_1 \subset \mathfrak{A}^{\rho-1}\mathfrak{a}$ and $d \neq 0$. This yields, for any valuation $B$ in $M$: $v_B(\alpha) \geqq \rho v_B(\phi_0)$, $v_B(\beta) = \rho v_B(\phi_0)$. Hence $v_B(\alpha/\beta) \geqq 0$, for all $B$ in $M$, and consequently $\alpha/\beta \subset \mathfrak{Z}^*$. This proves the first part of our theorem. Moreover, $\alpha/\beta$ is an element of $\mathfrak{P}_0$, if

and only if $v_B(\alpha) > v_B(\phi_0)$, i.e. if and only if $c = 0$, whence $\alpha \subset \mathfrak{A}^{\rho-1}\mathfrak{a}$. This proves the concluding assertion of the theorem.

To complete the proof, let $\xi$ be any element of $Q(P)$. The element $\xi$ can be written in the form of a quotient $f(\xi_1, \cdots, \xi_n)/\psi(\xi_1, \cdots, \xi_n)$, where $\psi(0, \cdots, 0) \neq 0$. By (19), we can then write $\xi$ in the form of a quotient $F(\phi_0, \phi_1, \cdots, \phi_n)/G(\phi_0, \phi_1, \cdots, \phi_n)$, where $F$ and $G$ are forms of the same degree, say $\rho$, and $G$ actually contains a term in $\phi_0^\rho$. Since all the $\phi$'s are in $\mathfrak{A}$, the elements $F$ and $G$ are in $\mathfrak{A}^\rho$. On the other hand, since all the power products of $\phi_0, \phi_1, \cdots, \phi_n$, of degree $\rho$, are elements of $\mathfrak{A}^{\rho-1}\mathfrak{a}$, *except* $\phi_0^\rho$, which is certainly not an element of $\mathfrak{A}^{\rho-1}\mathfrak{a}$, it follows that $G \not\equiv 0(\mathfrak{A}^{\rho-1}\mathfrak{a})$. This completes the proof of the theorem.

## 16

We shall conclude this part of the paper with a theorem concerning the factorization of the complete ideals $\mathfrak{A}$ and $\mathfrak{a}$ into simple $v$-factors (see $Z_1$). The notion of a simple $v$-ideal $\mathfrak{P}^{(h)}$, of kind $h$, is the arithmetic analog of the geometric concept of a point $A^{(h)}$ infinitely near $A$ and in the $(h-1)^{\text{th}}$ neighborhood of $A$. A given simple $v$-ideal $\mathfrak{P}^{(h)}$ determines uniquely a sequence $\mathfrak{P}^{(1)} = \mathfrak{p}_0, \mathfrak{P}^{(2)}, \cdots, \mathfrak{P}^{(h-1)}$ of simple $v$-ideals of kind $1, 2, \cdots, h-1$ respectively, such that if $B$ is any zero-dimensional valuation of $\Sigma$ whose valuation ring contains $\mathfrak{o}^*$ and for which $\mathfrak{P}^{(h)}$ is a $v$-ideal, then also the $\mathfrak{P}^{(i)}$, $i = 1, 2, \cdots, h-1$, are $v$-ideals belonging to $B$. Any of these $h-1$ simple $v$-ideals is called a *predecessor of* $\mathfrak{P}^{(h)}$. While the simple $v$-ideal $\mathfrak{P}^{(1)}$, of kind 1, corresponds to the proper point $A^{(1)} = A$, the other predecessors $\mathfrak{P}^{(i)}$ correspond to the points $A^{(2)}, \cdots, A^{(h-1)}$ which follow the point $A$ in the *first, second,* $\cdots$, $(h-2)^{\text{th}}$ neighborhood and which *precede* the point $A^{(h)}$.

A complete ideal can be factored into a product of simple $v$-ideals, and the factorization is unique (see $Z_1$, p. 172). Let

$$\mathfrak{A} = \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2} \cdots \mathfrak{P}_\mu^{\alpha_\mu},$$

$$\mathfrak{a} = \overline{\mathfrak{P}}_1^{\beta_1}\overline{\mathfrak{P}}_2^{\beta_2} \cdots \overline{\mathfrak{P}}_\nu^{\beta_\nu},$$

be the factorization of $\mathfrak{A}$ and $\mathfrak{a}$ respectively, into simple $v$-ideals. The individual simple $v$-factors in $\mathfrak{A}$ correspond to the effective base points of the ideal $\mathfrak{A}$, i.e. of the corresponding continuous system of curves $f = 0$, defined by the condition: $f \equiv 0(\mathfrak{A})$. The exponents $\alpha_i$ are related to the effective multiplicities of these curves at the base points.

In order to state the theorem which we wish to prove, we make the following remark. Let $\mathfrak{A}$ be exactly divisible by $\mathfrak{p}_0^\rho$ i.e. let $\mathfrak{A} \equiv 0(\mathfrak{p}_0^\rho)$, $\mathfrak{A} \not\equiv 0(\mathfrak{p}_0^{\rho+1})$. Since $\mathfrak{a} \equiv 0(\mathfrak{A})$, also $\mathfrak{a} \equiv 0(\mathfrak{p}_0^\rho)$. On the other hand, since $\mathfrak{A}\mathfrak{p}_0 \equiv 0(\mathfrak{a})$ (by Theorem 6), we have $\mathfrak{a} \not\equiv 0(\mathfrak{p}_0^{\rho+2})$. Hence $\mathfrak{a}$ is exactly divisible either by $\mathfrak{p}_0^\rho$ or by $\mathfrak{p}_0^{\rho+1}$. Our theorem is the following:

THEOREM 9. *If $\mathfrak{A}$ is exactly divisible by $\mathfrak{p}_0^\rho$ and $\mathfrak{a}$ is exactly divisible by $\mathfrak{p}_0^{\rho+1}$, then every simple v-factor $\overline{\mathfrak{P}}_i$ of $\mathfrak{a}$ is a predecessor of or coincides with some simple v-factor $\mathfrak{P}_j$ of $\mathfrak{A}$.*

PROOF.[18] Let $x$, $y$ be uniformizing parameters at $A$. The elements of $\mathfrak{o}^*$ are formal power series in $x$ and $y$. Every element $\alpha$ of $\mathfrak{a}$ is a power series $F_{\rho+1}(x, y) + F_{\rho+2}(x, y) + \cdots$, beginning with terms of degree $\rho + 1$ or higher. We call $F_{\rho+1}$ the *subform* of $\alpha$. As $\alpha$ varies in $\mathfrak{a}$, its subform varies in a linear system, of a certain dimension $r$ (a K-module of rank $r + 1$). Since $\mathfrak{p}_0\mathfrak{A} \equiv 0(\mathfrak{a})$, it follows immediately that $r \geqq 1$. This implies that $\mathfrak{p}_0$ must occur among the simple $v$-factors of $\mathfrak{a}$, since for any simple $v$-ideal of kind $> 1$ it is true that its system of subforms is of dimension zero ($Z_1$, p. 163, Corollary 3.2). We put into evidence the factor $\mathfrak{p}_0$ and we write $\mathfrak{a} = \mathfrak{p}_0\mathfrak{a}_1$. To prove our theorem, it will now be sufficient to prove that every simple $v$-factor in $\mathfrak{a}_1$ is a predecessor of, or coincides with, some simple $v$-factor of $\mathfrak{A}$. To prove this we first show that *the ideal* $\mathfrak{a}_1$ *coincides with the quotient* $\mathfrak{A}:\mathfrak{p}_0$.

Let $\mathfrak{A}:\mathfrak{p}_0 = \mathfrak{B}$. Since $\mathfrak{p}_0\mathfrak{a}_1 = \mathfrak{a} \equiv 0(\mathfrak{A})$, we have at any rate the inclusion

$$\mathfrak{a}_1 \subseteq \mathfrak{B}. \tag{22}$$

We assert that $\mathfrak{p}_0$ *does not occur as a factor in* $\mathfrak{A}$.[19] Since $\mathfrak{a}$ is a maximal subideal of $\mathfrak{A}$, it is clear that

$$\mathfrak{a} = [\mathfrak{A}, \mathfrak{p}_0^{\rho+1}]. \tag{23}$$

Let $ax + by$ be a fixed form which does not divide all subforms of $\mathfrak{A}$, and let $\mathfrak{P}_2' = (ax + by, \mathfrak{p}_0^3)$. The ideal $\mathfrak{P}_2'$ is a simple $v$-ideal of second kind. We consider the ideal $\Delta = [\mathfrak{A}, \mathfrak{p}_0^{\rho-1}\cdot\mathfrak{P}_2']$. Since $\mathfrak{p}_0^2 \equiv 0(\mathfrak{P}_2')$, we have, by (23): $\mathfrak{A} \supseteq \Delta \supseteq \mathfrak{a}$. By our choice of the form $ax + by$ it follows that $\mathfrak{A} \not\subseteq \mathfrak{p}_0^{\rho-1}\mathfrak{P}_2'$. Hence $\Delta \neq \mathfrak{A}$. Hence $\Delta = \mathfrak{a}$, since $\mathfrak{a}$ is a maximal subideal of $\mathfrak{A}$. Now suppose, if possible, that $\mathfrak{p}_0$ is a factor of $\mathfrak{A}$, and let $\mathfrak{A} = \mathfrak{p}_0\mathfrak{A}_1$, where $\mathfrak{A}_1$ is then necessarily exactly divisible by $\mathfrak{p}_0^{\rho-1}$. We have $\mathfrak{P}_2'\mathfrak{A}_1 \subseteq \mathfrak{P}_2'\mathfrak{p}_0^{\rho-1}$, and also $\mathfrak{P}_2'\mathfrak{A}_1 \subseteq \mathfrak{p}_0\mathfrak{A}_1 = \mathfrak{A}$. Hence $\mathfrak{P}_2'\mathfrak{A}_1 \subseteq \Delta$, i.e. $\mathfrak{P}_2'\mathfrak{A}_1 \subseteq \mathfrak{a}$. This is impossible, since $\mathfrak{P}_2'\mathfrak{A}_1$ is exactly divisible by $\mathfrak{p}_0^\rho$, while $\mathfrak{a}$ is divisible by $\mathfrak{p}_0^{\rho+1}$.

[18] It is not without interest to point out the intuitive geometric content of Theorem 9. Interpreted geometrically, Theorem 6 signifies that the complete ideal $\mathfrak{a}$ is obtained by imposing on $\mathfrak{A}$ *one* additional *base condition*, expressed by *one* linear relation. This base condition may be of a two-fold nature: (1) either we impose on the curves defined by $\mathfrak{A}$ the condition of passing through a *new base* point $A_{\rho+1}$, which *follows* immediately a sequence $A, A_1, \cdots, A_\rho$ of successive base points of $\mathfrak{A}$; (2) or we impose on these curves (which, in view of $\mathfrak{A} \equiv 0(\mathfrak{p}_0^\rho)$, already possess at $A$ an effective multiplicity $\rho$) the condition of possessing at $A$ a $\rho + 1$-fold point. In order that the new base condition be really equivalent to one linear condition, the following is necessary and sufficient: (1) in the first case, the branches of smallest order which pass through $A, A_1, \cdots, A_\rho$ and through $A, A_1, \cdots, A_{\rho+1}$ respectively, must have the same order (in the terminology of Enriques' theory: $A_{\rho+1}$ must be a free point, not a satellite); (2) in the second case, the general curve defined by $\mathfrak{A}$ must have all its $\rho$ tangents at $A$ fixed. In the first case, the new base condition will not lead automatically to an increased base multiplicity at $A$, and so $\mathfrak{a}$ will still be exactly divisible by $\mathfrak{p}_0^\rho$. In the second case $\mathfrak{a}$ will be exactly divisible by $\mathfrak{p}_0^{\rho+1}$, but—and this is the main point—this change in the effective multiplicity at $A$ may imply a lowering of the effective multiplicities at some other infinitely near base points, but *no new effective base points can appear*.

[19] In other words: the curves defined by elements of $\mathfrak{A}$ and having at $A$ exactly a $\rho$-fold point, have no variable tangent at $A$. Compare preceding footnote.

We come back to the quotient $\mathfrak{B} = \mathfrak{A}:\mathfrak{p}_0$. We have $\mathfrak{B} \equiv 0(\mathfrak{p}_0^{\rho-1})$. If we suppose that $\mathfrak{B}$ is exactly divisible by $\mathfrak{p}_0^{\rho-1}$, we would have a contradiction, since the relation $\mathfrak{B}\mathfrak{p}_0 \equiv 0(\mathfrak{A})$ would then imply that the system of subforms of $\mathfrak{A}$ is of dimension $\geqq 1$, whence $\mathfrak{p}_0$ would be a factor of $\mathfrak{A}$. Hence $\mathfrak{B}$ *is exactly divisible by* $\mathfrak{p}_0^{\rho}$. Hence $\mathfrak{B}\mathfrak{p}_0 \equiv 0(\mathfrak{p}_0^{\rho+1})$, and since $\mathfrak{B}\mathfrak{p}_0 \equiv 0(\mathfrak{A})$, it follows by (23), that $\mathfrak{p}_0\mathfrak{B} \equiv 0(\mathfrak{a})$, i.e. $\mathfrak{p}_0\mathfrak{B} \equiv 0(\mathfrak{p}_0\mathfrak{a}_1)$. In view of (22), we also have $\mathfrak{p}_0\mathfrak{a}_1 \equiv 0(\mathfrak{p}_0\mathfrak{B})$. Hence $\mathfrak{p}_0\mathfrak{a}_1 = \mathfrak{p}_0\mathfrak{B}$. Now both $\mathfrak{a}_1$ and $\mathfrak{B}$ are complete ideals: $\mathfrak{a}_1$ is a complete ideal, because it is a product of $v$-ideals ($Z_1$, p. 193); $\mathfrak{B}$ is a complete ideal because it is a quotient $\mathfrak{A}:\mathfrak{p}_0$ of a complete ideal $\mathfrak{A}$ and another ideal ($Z_1$, p. 193). In view of the unique factorization of complete ideals into simple $v$-factors, we conclude from the relation $\mathfrak{p}_0\mathfrak{a}_1 = \mathfrak{p}_0\mathfrak{B}$, that $\mathfrak{a}_1 = \mathfrak{B}$, i.e. $\mathfrak{a}_1 = \mathfrak{A}:\mathfrak{p}_0$. This proves our assertion.

We have pointed out above that in order to prove our theorem, we have only to prove that every simple $v$-factor of $\mathfrak{a}_1$ is the predecessor of, or coincides with, some simple $v$-factor of $\mathfrak{A}$. We now also know that $\mathfrak{a}_1 = \mathfrak{A}:\mathfrak{p}_0$. On this basis our theorem becomes a special case of the following general

LEMMA. *If $\mathfrak{A}$ is a zero-dimensional complete ideal in $\mathfrak{o}^*$ and if $\mathfrak{b}$ is any complete ideal, then every simple $v$-factor of the ideal $\mathfrak{B} = \mathfrak{A}:\mathfrak{b}$ is the predecessor of, or coincides with some simple $v$-factor of $\mathfrak{A}$.*

PROOF OF THE LEMMA. In view of the isomorphism between the zero-dimensional ideals of $\mathfrak{o}^*$ and those zero-dimensional primary ideals of the polynomial ring $\mathsf{K}[x, y]$ which belong to the ideal $(x, y)$, it is sufficient to prove the lemma for polynomial rings. We assume therefore that $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{b}$ are ideals in the polynomial ring $\mathfrak{o} = \mathsf{K}[x, y]$. Let $\mathfrak{A} = \mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_\mu^{\alpha_\mu}$, and let $\mathfrak{P}_i$ be of kind $h_i$. Let $h = \max(h_1, \cdots, h_\mu)$. The lemma is trivial for $h = 1$. In fact, if $h = 1$, then $\mathfrak{P}_1, \cdots, \mathfrak{P}_\mu$ are distinct prime zero-dimensional ideals, and it is obvious that $\mathfrak{A}:\mathfrak{b}$ will be of the form $\mathfrak{P}_1^{\beta_1} \cdots \mathfrak{P}_\mu^{\beta_\mu}$, $\beta_i \leqq \alpha_i$. We therefore prove the lemma by induction with respect to $h$. We assume that the lemma is true for $h < g$, and we prove that it is true for $h = g$. First of all, we observe that it is sufficient to prove the lemma for $h = g$, under the hypothesis that the simple $v$-factors $\mathfrak{P}_1, \cdots, \mathfrak{P}_\mu$ of $\mathfrak{A}$ all belong to one and the same prime zero-dimensional ideal $\mathfrak{p}_0$, say $\mathfrak{p}_0 = (x, y)$. Namely, in the general case we can write $\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \cdots \mathfrak{A}_\tau = [\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_\tau]$, where the $\mathfrak{A}_i$ are complete ideals belonging to *distinct* prime zero-dimensional ideals. Then we will have $\mathfrak{A}:\mathfrak{b} = [\mathfrak{A}_1:\mathfrak{b}, \cdots, \mathfrak{A}_\tau:\mathfrak{b}] = (\mathfrak{A}_1:\mathfrak{b}) \cdots (\mathfrak{A}_\tau:\mathfrak{b})$. If the Lemma is true for each factor $\mathfrak{A}_i:\mathfrak{b}$, it is also true for the product $\mathfrak{A}:\mathfrak{b}$.

We assume then that $\mathfrak{P}_1, \cdots, \mathfrak{P}_\mu$ belong to the prime ideal $\mathfrak{p}_0 = (x, y)$. Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{b}$ be exactly divisible by $\mathfrak{p}_0^{\rho}$, $\mathfrak{p}_0^{\sigma}$, $\mathfrak{p}_0^{\tau}$ respectively. Since $\mathfrak{B}\mathfrak{b} \equiv 0(\mathfrak{A})$, we must have $\sigma + \tau \geqq \rho$. Replacing, if necessary, $x$ by a linear form $ax + by$ with non-special coefficients, we may assume that the subform of $\mathfrak{P}_i$ ($i = 1, 2, \cdots, \mu$) is not a power of $x$ (i.e. the line $x = 0$ is not the tangent line of the branches of lowest order defined by $\mathfrak{P}_i$). Under this condition, the transform of $\mathfrak{P}_i$ by the quadratic transformation

$$x' = x, y' = y/x$$

is a simple $v$-ideal $\mathfrak{P}_i'$ in $\mathfrak{o}' = \mathsf{K}[x', y']$, of kind $h_i - 1$ ($Z_1$, p. 169). Let

$$\mathfrak{o}' \cdot \mathfrak{A} = x^{\rho}\mathfrak{A}', \qquad \mathfrak{o}'\mathfrak{B} = x^{\sigma}\mathfrak{B}', \qquad \mathfrak{o}'\mathfrak{b} = x^{\tau}\mathfrak{b}', \tag{24}$$

where $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{b}'$ are again complete ideals in $\mathfrak{o}'$ ($Z_1$, p. 196), and $\mathfrak{A}'$, $\mathfrak{B}'$ are zero-dimensional. By hypothesis, $g = \max(h_i)$. Hence $\max(h_i - 1) < g$ and, by our induction, the lemma is true for $\mathfrak{A}'$. *We prove that*

$$\mathfrak{B}' = \mathfrak{A}' : x^{\sigma+\tau-\rho}\mathfrak{b}'. \tag{25}$$

From this our lemma will follow, since the simple $v$-factors of $\mathfrak{B}'$ are the transforms of the simple $v$-factors of $\mathfrak{B}$ different from $\mathfrak{p}_0$.

Since $\mathfrak{B}\mathfrak{b} \equiv 0(\mathfrak{A})$, we have, by (24), $x^{\sigma+\tau-\rho}\mathfrak{B}'\mathfrak{b}' \equiv 0(\mathfrak{A}')$, whence

$$\mathfrak{B}' \subseteq \mathfrak{A}' : x^{\sigma+\tau-\rho}\mathfrak{b}'. \tag{26}$$

Let $\mathfrak{A}' : x^{\sigma+\tau-\rho}\mathfrak{b}' = \mathfrak{B}_1'$, and let $x^q$ be the lowest power of $x$ such that $x^q\mathfrak{B}_1'$ is the extended ideal of an ideal in $\mathfrak{o}$. Then $x^q\mathfrak{B}_1'$ is also the extended ideal of its contracted ideal ($Z_1$, p. 196) in $\mathfrak{o}$. Let $\mathfrak{B}_1$ be the contracted ideal. From the relation $\mathfrak{B}' \subseteq \mathfrak{B}_1'$ follows the inequality $q \leqq \sigma$ (see $Z_1$, p. 199). We have $\mathfrak{o}'\mathfrak{B}_1 = x^q\mathfrak{B}_1'$, hence $\mathfrak{o}'\mathfrak{p}_0^{\sigma-q}\mathfrak{B}_1 = x^{\sigma}\mathfrak{B}_1'$. Since $\mathfrak{B}$ and $\mathfrak{p}_0^{\sigma-q}\mathfrak{B}_1$ are the contracted ideals of $x^{\sigma}\mathfrak{B}'$ and $x^{\sigma}\mathfrak{B}_1'$ respectively, and since $\mathfrak{B}' \subseteq \mathfrak{B}_1'$ (by (26)), we conclude that

$$\mathfrak{B} \subseteq \mathfrak{p}_0^{\sigma-q}\mathfrak{B}_1. \tag{27}$$

On the other hand, we have $x^{\sigma+\tau-\rho}\mathfrak{b}'\mathfrak{B}' \equiv 0(\mathfrak{A}')$, whence $x^{\sigma+\tau}\mathfrak{b}'\mathfrak{B}' \equiv 0(x^{\rho}\mathfrak{A}')$. Now $x^{\sigma+\tau}\mathfrak{b}'\mathfrak{B}_1'$ is the extended ideal of $\mathfrak{p}_0^{\sigma-q}\mathfrak{b}\mathfrak{B}_1$. Hence, passing to the contracted ideals, we find: $\mathfrak{p}_0^{\sigma-q}\mathfrak{b}\mathfrak{B}_1 \subseteq \mathfrak{A}$, i.e.

$$\mathfrak{p}_0^{\sigma-q}\mathfrak{B}_1 \subseteq \mathfrak{B}. \tag{27'}$$

Comparing (27) and (27'), we conclude that $\mathfrak{p}_0^{\sigma-q}\mathfrak{B}_1 = \mathfrak{B}$. Passing to the extended ideals in $\mathfrak{o}'$, we have $\mathfrak{B}_1' = \mathfrak{B}'$, i.e. (25), q.e.d.

## V. Normal Sequences of Integrally Closed Quotient Rings. "Local Reduction" Theorem

### 17. Tangential ideals

Let $F$, a projective model of our field $\Sigma$, be given in an affine $S_n(x_1, \cdots, x_n)$ by the ring $\mathfrak{J} = \mathsf{K}[\xi_1, \cdots, \xi_n]$. We consider a point $P$ on $F$ and its quotient ring $\mathfrak{J}^* = Q(P)$. We assume that $P$ is at finite distance, say at the origin $x_1 = \cdots = x_n = 0$. Let $\mathfrak{p}_0 = \mathfrak{J} \cdot (\xi_1, \cdots, \xi_n)$, $\mathfrak{p}_0^* = \mathfrak{J}^* \cdot \mathfrak{p}_0$, be the corresponding prime zero-dimensional ideals in $\mathfrak{J}$ and $\mathfrak{J}^*$ respectively.

The surface $F$ possesses at $P$ a *tangent cone*. We ask: what is, from an arithmetic standpoint, a tangent line of $F$ at $P$? First of all, any line $l$ through $P$ (tangent or not) can be described by the system of hyperplanes which contain it. They are the hyperplanes $u_1x_1 + \cdots + u_nx_n = 0$, where the coefficients $u_i$ satisfy a given linear relation $c_1u_1 + \cdots + c_nu_n = 0$, $c_i \subset \mathsf{K}$. Any element $\xi$ in $\mathfrak{p}_0$ is a polynomial in $\xi_1, \cdots, \xi_n$, in which the constant term is missing: $\xi = a_1\xi_1 + \cdots + a_n\xi_n +$ terms of higher degree. The elements $\xi$ such that

the coefficients $a_i$ satisfy the relation $c_1a_1 + \cdots + c_na_n = 0$ form a *primary maximal subideal* $\mathfrak{q}$ of $\mathfrak{p}_0$. We associate the ideal $\mathfrak{q}$ with the line $l$. The corresponding ideal in $\mathfrak{J}^*$ shall be denoted by $\mathfrak{q}^*$. Conversely, given a maximal primary subideal $\mathfrak{q}$ of $\mathfrak{p}_0$, the ring $\mathfrak{p}_0/\mathfrak{q}$ is a K-module of rank 1. Hence $\mathfrak{q}$ consists of all those elements $\xi = a_1\xi_1 + \cdots + a_n\xi_n + \cdots$ of $\mathfrak{p}_0$, in which the $a_i$ satisfy a linear relation $c_1a_1 + \cdots + c_na_n = 0$. The hyperplanes $u_1x_1 + \cdots + u_nx_n = 0$ whose coördinates $u_i$ satisfy the relation $c_1u_1 + \cdots + c_nu_n = 0$ have in common a line $l$ through $P$. The line $l$ corresponds to the ideal $\mathfrak{q}$ in $\mathfrak{J}$ (or $\mathfrak{q}^*$ in $\mathfrak{J}^*$).

Now let $l$ be a *tangent line*. We can think of $l$ as the tangent line of some branch $\gamma$ (for instance, an algebraic branch) which lies on $F$ and has origin at $P$. The branch $\gamma$ defines a zero-dimensional valuation $B$ of the field $\Sigma$, and $P$ is the center of $B$ on $F$. The elements $\xi_1, \cdots, \xi_n$ have positive values in $B$. It is clear that if $\xi$ is any element in $\mathfrak{p}_0$, or in $\mathfrak{p}_0^*$, then $v_B(\xi) \geqq \min\{v_B(\xi_1), \cdots, v_B(\xi_n)\}$, whence $v_B(\mathfrak{p}_0) = v_B(\mathfrak{p}_0^*) = \min\{v_B(\xi_1), \cdots, v_B(\xi_n)\}$. The elements $\xi$ of $\mathfrak{p}_0^*$, such that $v_B(\xi) > v_B(\mathfrak{p}_0)$, form a primary subideal $\mathfrak{q}^*$ of $\mathfrak{p}_0^*$, since $\mathfrak{J}^*$ is contained in the valuation ring of $B$. Let $\eta$ be an element in $\mathfrak{p}_0^*$, not in $\mathfrak{q}^*$. If $\eta_1$ is any element in $\mathfrak{p}_0^*$, then $v_B(\eta_1/\eta) \geqq 0$. Since $B$ is zero-dimensional, there exists a constant $c$ such that $v_B(\eta_1/\eta - c) > 0$, i.e. $\eta_1 - c\eta \equiv 0(\mathfrak{q}^*)$. This shows that the ring of residual classes $\mathfrak{p}_0^*/\mathfrak{q}^*$ is a K-module of rank 1, and hence $\mathfrak{q}^*$ is a maximal subideal of $\mathfrak{p}_0^*$. The line $l$ associated with $\mathfrak{q}^*$ shall be, by definition, the tangent line of the branch $\gamma$.

A maximal primary subideal $\mathfrak{q}^*$ of $\mathfrak{p}_0^*$ (or the corresponding subideal $\mathfrak{q}$ of $\mathfrak{p}_0$) which corresponds to a tangent line, shall be called a *tangential ideal of* $Q(P)$. From the standpoint of valuation theory, a tangential ideal $\mathfrak{q}^*$ is characterized by the following two properties: (1) $\mathfrak{q}^*$ is a valuation ideal belonging to some zero-dimensional valuation of center $P$; (2) $\mathfrak{q}^*$ is a maximal subideal of $\mathfrak{p}_0^*$.

### 18. Tangential ideals and quadratic transformations

Let $y_0, y_1, \cdots, y_n$ be homogeneous coördinates in $S_n$, $x_i = y_i/y_0$, $i = 1, 2, \cdots, n$. We consider the quadratic transformation:

$$\begin{aligned} \rho y_{0j} &= y_0y_j, & i, j &= 1, 2, \cdots, n, \\ \rho y_{ij} &= y_iy_j, & y_{ij} &= y_{ji}, \end{aligned} \tag{28}$$

where we interpret the $\frac{1}{2}(n+1)(n+2) - 1$ $y_{ij}$'s as homogeneous coördinates in a projective $P_N$, $N = \frac{1}{2}(n+1)(n+2) - 2$. The transformation (28) carries the system of hyperquadrics of $S_n$ which pass through the point $P(y_0 = 1, y_1 = \cdots = y_n = 0)$ into the system of hyperplanes of $P_N$.

Let $\omega_0, \omega_1, \cdots, \omega_n$ be the homogeneous coördinates of the general point of $F$. Here $\omega_0$ is a transcendental quantity over the field $\Sigma$, and $\omega_i/\omega_0 = \xi_i$. The elements

$$\begin{aligned} \omega_{0j} &= \omega_0\omega_j, & i, j &= 1, 2, \cdots, n, \\ \omega_{ij} &= \omega_i\omega_j, \end{aligned} \tag{29}$$

can be regarded as the homogeneous coördinates of the general point of a surface $F'$ birationally equivalent to $F$ and lying in $P_N$. The surface $F'$ is *the transform of $F$ by the quadratic transformation* (18.) In the system of non-homogeneous coördinates $x_{ij}^{(\nu)} = y_{ij}/y_{0\nu}$, $\nu$-fixed, the non-homogeneous coördinates of the general point of $F'$ are

$$\begin{aligned} \xi_{0j}^{(\nu)} &= \xi_j/\xi_\nu, & j &= 1, 2, \cdots, \nu-1, \nu+1, \cdots, n, \\ \xi_{ij}^{(\nu)} &= \xi_i\xi_j/\xi_\nu, & i, j &= 1, 2, \cdots, n, \end{aligned} \tag{30}$$

and we have

$$\mathsf{K}[\xi_{ij}^{(\nu)}] = \mathsf{K}[\xi_\nu, \xi_1/\xi_\nu, \cdots, \xi_{\nu-1}/\xi_\nu, \xi_{\nu+1}/\xi_\nu, \cdots, \xi_n/\xi_\nu] = \mathfrak{J}^{(\nu)}. \tag{30'}$$

Let $A$ be a point on $F$ different from $P$, and let $y_0 = b_0$, $y_1 = b_1$, $y_n = b_n$ be the homogeneous coördinates of $A$, where $b_1, \cdots, b_n$ are not all zero. Let, for instance, $b_n \neq 0$. If we choose as non-homogeneous coördinates in $P_n$ the ratios $x_i^* = y_i/y_n$ $i = 0, 1, \cdots, n-1$, then the point $A$ will be at finite distance and will have coördinates $x_i^* = a_i = b_i/b_n$. In this system of coördinates, the coördinates of the general point of $F$ are the elements $1/\xi_n$, $\xi_1/\xi_n, \cdots, \xi_{n-1}/\xi_n$, giving rise to the ring

$$\mathfrak{J}_n = \mathsf{K}[1/\xi_n, \xi_1/\xi_n, \cdots, \xi_{n-1}/\xi_n].$$

Let us choose as non-homogeneous coördinates in $P_N$ the ratios $x_{ij}^* = y_{ij}/y_{nn}$. The coördinates $\xi_{ij}^*$ of the general point of $F'$ will then be the elements:

$$\xi_{0j}^* = \frac{1}{\xi_n}\cdot\frac{\xi_j}{\xi_n}, \qquad \xi_{ij}^* = \frac{\xi_i}{\xi_n}\cdot\frac{\xi_j}{\xi_n}, \quad i, j = 1, 2, \cdots, n-1;$$

$$\xi_{0n}^* = \frac{1}{\xi_n}, \qquad \xi_{in}^* = \frac{\xi_i}{\xi_n}, \qquad i = 1, 2, \cdots, n-1.$$

The ring $\mathsf{K}[\xi_{ij}^*]$ coincides with $\mathfrak{J}_n$. Hence to every point $A$ of $F$ at which the $x_i^*$ are finite, there corresponds a point $A'$ on $F'$ at which the $x_{ij}^*$ are finite, *and the quotient rings of the two corresponding points coincide.* From the coincidence of the quotient rings $Q(A)$, $Q(A')$ follows that *$A'$ is the only point of $F'$ which corresponds to $A$, and vice versa* (see IV, 14). *This, and the invariance of the quotient ring $Q(A)$, holds then for every point $A$ of $F$ which is different from $P$.*

Let now $P'$ be a point of $F'$ which corresponds to $P$. There must exist then a zero-dimensional valuation $B$ of $\Sigma$ whose center on $F$ is $P$ and whose center on $F'$ is $P'$. The elements $\xi_1, \cdots, \xi_n$ have positive values in $B$. Let $\xi_\nu$ be one of the $\xi$'s for which $v_B(\xi_\nu) = \min(v_B(\xi_1), \cdots, v_B(\xi_n))$. Then $v_B(\xi_i/\xi_\nu) \geqq 0$, $i \neq \nu$. Hence, in view of (30), the point $P'$, in the system of non-homogeneous coördinates $x_{ij}^{(\nu)}$, is a point at a finite distance. It is therefore given by a prime zero-dimensional ideal $\mathfrak{p}_0^{(\nu)}$ in the ring $\mathfrak{J}^{(\nu)}$ of (30'). This ideal must be a divisor of the principal ideal $\mathfrak{J}^{(\nu)}\cdot\xi_\nu$, since $v_B(\xi_\nu) > 0$. The point $P'$ therefore

belongs to the curve $\Gamma^{(\nu)}$ defined on $F'$ by the principal ideal $\mathfrak{J}^{(\nu)} \cdot \xi_\nu$.[20] Conversely, let $P'$ be any point of $\Gamma^{(\nu)}$, and at finite distance with respect to the non-homogeneous coördinates $x_{ij}^{(\nu)}$. If $B$ is a zero-dimensional valuation whose center is $P'$, then $v_B(\xi_\nu) > 0$, $v_B(\xi_i/\xi_\nu) \geqq 0$, $i \neq \nu$. Hence $v_B(\xi_i) > 0$, $i = 1, 2, \cdots, n$, and therefore the center of $B$ on $F$ is the point $P$. Consequently, *every irreducible component of* $\Gamma^{(\nu)}$ *is a fundamental curve which corresponds to* $P$ (see IV, 14, theorem 4) *and if* $P'$ *is any point of* $\Gamma^{(\nu)}$, $P$ *is the only point which corresponds to* $P'$.

It is clear that the relationship between the curves $\Gamma^{(1)}, \Gamma^{(2)}, \cdots, \Gamma^{(n)}$ is simply the following: an irreducible component of a $\Gamma^{(i)}$, $i \neq \nu$, which does not belong to $\Gamma^{(\nu)}$, is necessarily, in the system of non-homogeneous coördinates $x_{ij}^{(\nu)}$, a curve at infinity. It is also not difficult to see that the entire fundamental curve $\Gamma = \Gamma^{(1)} + \cdots + \Gamma^{(n)}$ is given in the ring $K[\omega_{ij}]$ by the *homogeneous* 1-dimensional ideal $(\omega_{11}, \omega_{12}, \cdots, \omega_{nn})$.

We go back to the point $P'$ on $\Gamma^{(\nu)}$ considered above and to the corresponding prime zero-dimensional ideal $\mathfrak{p}_0^{(\nu)}$ in $\mathfrak{J}^{(\nu)}$. Let

$$\mathfrak{p}_0^{(\nu)} = \mathfrak{J}^{(\nu)} \cdot (\xi_\nu, \xi_1/\xi_\nu - c_1, \cdots, \xi_{\nu-1}/\xi_\nu - c_{\nu-1}, \cdots, \xi_{\nu+1}/\xi_\nu - c_{\nu+1}, \cdots, \xi_n/\xi_\nu - c_n). \tag{31}$$

If $B$ is any zero-dimensional valuation whose center is $P'$, then

$$v_B(\xi_i - c_i\xi_\nu) > v_B(\xi_\nu), \qquad i \neq \nu.$$

For all such valuations, the corresponding tangential ideal $\mathfrak{q}^*$ in the quotient ring $Q(P)$, is one and the same, namely:

$$\mathfrak{q}^* = \mathfrak{J}^* \cdot (\xi_1 - c_1\xi_\nu, \cdots, \xi_{\nu-1} - c_{\nu-1}\xi_\nu, \xi_{\nu+1} - c_{\nu+1}\xi_\nu, \cdots, \xi_n - c_n\xi_\nu, \mathfrak{p}_0^{*2}). \tag{32}$$

Hence, *every point* $P'$ *which corresponds to* $P$ *determines uniquely a tangential ideal* $\mathfrak{q}^*$ in $Q(P)$. The relationship between $P'$ and $\mathfrak{q}^*$ is such that, if $B$ is any zero-dimensional valuation with center at $P'$, then $\mathfrak{q}^*$ is a valuation ideal of $B$ in $Q(P)$ (namely, $\mathfrak{q}^*$ is the ideal consisting of all those elements of $Q(P)$ whose value is greater than $v_B(\mathfrak{p}_0^*)$). That, conversely, every tangential subideal of $\mathfrak{p}_0^*$ determines a point $P'$ which corresponds to $P$, is obvious, in view of our definition of a tangential ideal in terms of zero-dimensional valuations. We conclude that *there is a* (1, 1) *correspondence between the points* $P'$ *of the entire fundamental curve* $\Gamma$ *and the tangential ideals of* $Q(P)$.

We now wish to elucidate the relationship between the quotient ring $\mathfrak{J}^* = Q(P)$ and the quotient ring $\mathfrak{J}'^* = Q(P')$ of a point $P'$ of the fundamental curve. We assume, as above, that $P'$ is on $\Gamma^{(\nu)}$, at finite distance. We observe first of all that the ring $\mathfrak{J} = \mathsf{K}[\xi_i]$ is a subring of $\mathfrak{J}^{(\nu)}$, as is seen immediately from (30′). Hence, also $\mathfrak{J}^*$ is a subring of $\mathfrak{J}'^*$. Moreover,

$$\mathfrak{J}^{(\nu)} \cdot \mathfrak{p}_0 = \mathfrak{J}^{(\nu)} \cdot (\xi_1, \cdots, \xi_n) = \mathfrak{J}^{(\nu)} \cdot \xi_\nu,$$

[20] It is well known that any principal ideal in $\mathfrak{J}^{(\nu)}$, different from the unit ideal, is one-dimensional, and its prime zero-dimensional components are all imbedded.

and, correspondingly,

$$\mathfrak{J}'^{*}\cdot\mathfrak{p}_0 = \mathfrak{J}'^{*}\cdot\xi_\nu . \tag{33}$$

We also point out the relation:

$$\mathfrak{J}'^{*}\cdot\mathfrak{q}^{*} = \xi_\nu\cdot\mathfrak{p}_0^{*(\nu)}, \tag{33'}$$

where $\mathfrak{p}_0^{*(\nu)}$ is the prime zero-dimensional ideal of the quotient ring $Q(P')$. This follows from (31) and (32).

Without loss of generality we may assume that the constants $c_1, \cdots, c_{\nu-1}, c_{\nu+1}, \cdots, c_n$ in (31) are all zero. Then (32) becomes

$$\mathfrak{q}^{*} = (\xi_1, \cdots, \xi_{\nu-1}, \xi_{\nu+1}, \cdots, \xi_n, \mathfrak{p}_0^{*2}). \tag{34}$$

If we put $\xi_i/\xi_\nu = \xi_i'$, $i \neq \nu$, $\xi_\nu = \xi_\nu'$, then any element $\eta'$ of $Q(P')$ is a quotient of two polynomials $f(\xi_1', \cdots, \xi_n')/g(\xi_1', \cdots, \xi_n')$, with the condition $g(0, \cdots, 0) = 0$. Returning to the elements $\xi$, we see that $\eta'$ is of the form:

$$\eta' = \frac{F(\xi)}{G(\xi)} = \frac{F_\rho(\xi) + F_{\rho+1}(\xi) + \cdots}{G_\rho(\xi) + G_{\rho+1}(\xi) + \cdots}, \tag{35}$$

where $F_i$, $G_i$ are forms of degree $i$ in $\xi_1, \cdots, \xi_n$, with the condition:

$$G_\rho = d\cdot\xi_\nu^{\rho} + \cdots \qquad d \neq 0. \tag{35'}$$

Conversely, every quotient $\eta'$ such as in (35), for which (35') holds true, is an element of $Q(P')$, as can be seen immediately if both $F$ and $G$ are divided through by $\xi_\nu^{\rho}$. It is clear that both $F$ and $G$ are elements of $\mathfrak{p}_0^{*\rho}$. In view of (34), the inequality $d \neq 0$ in (35') is certainly satisfied if $G \not\equiv 0(\mathfrak{p}_0^{*\rho-1}\mathfrak{q}^{*})$. Conversely, let us assume that $d \neq 0$. Then $G \equiv 0(\mathfrak{p}_0^{*\rho-1}\mathfrak{q}^{*})$ would imply that $\xi_\nu^{\rho}$ is in $\mathfrak{p}_0^{*\rho-1}\cdot\mathfrak{q}^{*}$. This is impossible, since if $B$ is any zero-dimensional valuation with center of $P'$, then $v_B(\mathfrak{q}^{*}) > v_B(\xi_\nu)$.[21]

It follows that $G \not\equiv 0(\mathfrak{p}_0^{*\rho-1}\mathfrak{q}^{*})$ *is equivalent to the condition* (35'). In a similar fashion it follows that $\eta'$ belongs to the prime zero-dimensional ideal of $Q(P')$, if and only if $F \equiv 0(\mathfrak{p}^{*\rho-1}\mathfrak{q}^{*})$.

For convenience we reassume the results of this section:

*The quadratic transformation* (28) (or (29)) *carries our surface $F$ into a birationally equivalent surface $F'$. With the exception of the fundamental point $P$ on $F$, the correspondence between the points of $F$ and $F'$ is strictly one-to-one, and there is invariance of quotient rings of corresponding points. To the point $P$ there corresponds a fundamental curve $\Gamma$, and we have $Q(P) \subset Q(P')$ for every point $P'$ on $\Gamma$. The points $P'$ on $\Gamma$ are in* (1, 1) *correspondence with the tangential ideals*

[21] This reasoning shows that $\mathfrak{p}_0^{*\rho} \not\equiv \mathfrak{p}_0^{*\rho-1}\mathfrak{q}^{*}$, for all $\rho$. It is not difficult to show that *these inequalities, together with the condition that $\mathfrak{q}^{*}$ be a maximal subideal of $\mathfrak{p}_0^{*}$, characterize tangential ideals.* Namely, assuming that $\mathfrak{q}^{*}$ is given by (34), it is a straightforward matter to show that the above inequalities imply that the ideal $(\xi_\nu, \xi_1/\xi_\nu, \cdots, \xi_{\nu-1}/\xi_\nu, \xi_{\nu+1}/\xi_\nu, \cdots, \xi_n/\xi_\nu)$ in $\mathfrak{J}^{(\nu)}$ is necessarily zero-dimensional (and not the unit ideal). The point $P'$ defined by this ideal is on $\Gamma^{(\nu)}$ and $\mathfrak{q}^{*}$ is the corresponding tangential ideal.

*in $Q(P)$. The correspondence is such that if to $P'$ corresponds the tangential ideal $\mathfrak{q}^*$, then the quotient ring $Q(P')$ consists of all quotients $\frac{F}{G}$, $F, G \subset Q(P)$, such that: if $G$ is exactly divisible by $\mathfrak{p}_0^{*\rho}$ (i.e. if $G \equiv 0(\mathfrak{p}_0^{*\rho})$, $G \not\equiv 0(\mathfrak{p}_0^{*\rho+1})$), then $G \not\equiv 0(\mathfrak{p}_0^{*\rho-1}\mathfrak{q}^*)$ and $F \equiv 0(\mathfrak{p}_0^{*\rho})$. The prime zero-dimensional ideal of $Q(P')$ consists of all the above quotients $\frac{F}{G}$ in which the numerator satisfies the additional condition: $F \equiv 0(\mathfrak{p}_0^{*\rho-1}\mathfrak{q}^*)$.*

The above description of the quotient ring $Q(P')$ is very similar to the one given in Theorem 8 in a different connection. The ideals $\mathfrak{p}_0^*$ and $\mathfrak{q}^*$ now play the rôle of $\mathfrak{A}$ and $\mathfrak{a}$ respectively.

### 19. Normal sequences of quotient rings

We have seen in the preceding section that the quotient ring $Q(P')$ of a point $P'$ on the fundamental curve can be fully described in terms of $Q(P)$ and of a tangential ideal $\mathfrak{q}^*$ in $Q(P)$. The operation consisting in passing from $Q(P)$ to $Q(P')$ is therefore an intrinsic operation on the quotient ring $Q(P)$. The quadratic transformation (28), (or (29)), is only *a projective realization* of this operation. Nevertheless, we shall continue to say that $Q(P')$ *is obtained from $Q(P)$ by a quadratic transformation.* There are as many *distinct* quotient rings obtainable from $Q(P)$ by a quadratic transformation, as there are tangential ideals in $Q(P)$.

Let us now assume that $Q(P)(=\mathfrak{J}^*)$ is integrally closed. Then it is quite possible that $\mathfrak{J}' = Q(P')$ is not integrally closed.[22] Let $\overline{\mathfrak{J}}'$ be the integral closure of $\mathfrak{J}'$. The prime zero-dimensional ideal of $\mathfrak{J}'$ may split up in $\overline{\mathfrak{J}}'$ into a finite number of distinct prime zero-dimensional ideals. Let $\mathfrak{p}_0'$ be one of them, and let $\mathfrak{J}_1^* = \overline{\mathfrak{J}}'_{\mathfrak{p}_0'}$ be the corresponding quotient ring. The quotient ring $\mathfrak{J}_1^*$ is again integrally closed and possesses only one prime zero-dimensional ideal. We shall say that $\mathfrak{J}_1^*$ *is obtained from $\mathfrak{J}^*$ by a quadratic transformation followed by integral closure.* It is quite clear that $\mathfrak{J}_1^*$ can be actually realized as the quotient ring of a point on some projective model of $\Sigma$. Namely, if $F'$ is the transform of $F$ by the quadratic transformation of the preceding section, and if $F_1$ is one of the normal surfaces determined by $F'$, then $\mathfrak{J}_1^*$ is the quotient ring $Q(P_1)$ of a point $P_1$ on $F_1$.

[22] Example: Let $P$ be the point $x = y = z = 0$ on the surface $z^2 = x^4 + y^4$. Apply the quadratic transformation $x' = x$, $y' = \frac{y}{x}$, $z' = \frac{z}{x}$ (i.e. pass to the ring $\mathfrak{J}^{(1)}$, given in (30′), where $\xi_1 = x$, $\xi_2 = y$, $\xi_3 = z$). The transformed surface $z'^2 = x'^2(1 + y'^4)$ has a multiple line $x' = z' = 0$ (the fundamental line of the transformation). Hence while the ring $\mathsf{K}[x, y, z]$ is integrally closed, the ring $\mathsf{K}[x', y', z']$ is not (for instance $\frac{z'}{x'}$ is integrally dependent on $\mathsf{K}[x', y']$.) It is clear that if $P'$ is any point on the line $x' = z' = 0$, the quotient ring $Q(P')$ is not integrally closed. More generally, whenever the fundamental curve $\Gamma$ on $F'$, created by the quadratic transformation, is a multiple curve, the quotient ring $Q(P')$ of any point on $\Gamma$ will not be integrally closed.

We say that an infinite sequence of quotient rings

$$\mathfrak{J}^* = Q(P), \qquad \mathfrak{J}_1^* = Q(P_1), \qquad \mathfrak{J}_2^* = Q(P_2), \cdots,$$

is a *normal sequence* if: (1) each $Q(P_i)$ is the quotient ring of a point $P_i$ on some normal projective model $F_i$ of our field $\Sigma$; (2) and if $Q(P_{i+1})$ is obtained from $Q(P)_i$ by a quadratic transformation followed by integral closure.

Let $\Omega = \lim_{i\to\infty} \mathfrak{J}_i^*$ be the *limit ring* of the rings $\mathfrak{J}_i^*$, i.e. the union of the rings $\mathfrak{J}_i^*$.

THEOREM 10. *The limit ring $\Omega$ of a normal sequence of quotient rings is the valuation ring of a zero-dimensional valuation of $\Sigma$.*

PROOF. We first show that there *cannot exist a one-dimensional valuation $B_1$ of $\Sigma$ with these two properties*: (1) *the valuation ring of $B_1$ contains $\Omega$*; (2) *$B_1$ is of second kind with respect to each ring $\mathfrak{J}_i^*$*. In fact, let $B_1$ be any one-dimensional valuation of $\Sigma$. Since $B_1$ is one-dimensional, we can find an element $\alpha$ in the valuation ring of $B_1$ such that $\alpha$ is not congruent to a constant modulo the prime ideal of $B_1$. Let $\alpha = \xi/\eta$, $\xi, \eta \subset Q(P)$, and let us assume that $B_1$ is of second kind with respect to $\mathfrak{J}^*$, i.e., that the contracted ideal in $\mathfrak{J}^*$ of the prime ideal of $B_1$ is the prime zero-dimensional $\mathfrak{p}^*$ of $\mathfrak{J}^*$ (we denote, more generally, the prime zero-dimensional ideal of $\mathfrak{J}_i^*$ by $\mathfrak{p}_i^*$). Under this hypothesis, $\alpha$ is not in $Q(P)$, since every element of $Q(P)$ is congruent to a constant mod $\mathfrak{p}^*$. Hence $\eta \equiv 0(\mathfrak{p}^*)$, whence also $\xi \equiv 0(\mathfrak{p}^*)$, since $v_{B_1}(\alpha) \geqq 0$. Now let $\mathfrak{q}^*$ be the tangential ideal in $\mathfrak{J}^*$ determined by the quotient ring $\mathfrak{J}_1^*$ (or rather by the intermediate quotient ring $\mathfrak{J}'$ which was obtained from $\mathfrak{J}$ by a quadratic transformation and from which $\mathfrak{J}_1^*$ is obtained by the operation of integral closure). Let $\zeta$ be an element in $\mathfrak{p}^*$, but not in $\mathfrak{q}^*$. Then $\xi/\zeta$ and $\eta/\zeta$ are elements of $\mathfrak{J}'$, and hence also of $\mathfrak{J}_1^*$. Let then $\xi = \zeta\xi_1$, $\eta = \zeta\eta_1$, $\xi_1, \eta_1 \subset \mathfrak{J}_1^*$. Since $B_1$ is of second kind with respect to $\mathfrak{J}^*$, we have $v_{B_1}(\zeta) > 0$, whence $v_{B_1}(\xi) > v_{B_1}(\xi_1)$, $v_{B_1}(\eta) > v_{B_1}(\eta_1)$, and $\alpha = \xi_1/\eta_1$.

Now, in a similar fashion, if we assume that $B_1$ is of second kind with respect to $\mathfrak{J}_1^*$, then we can write $\alpha = \xi_2/\eta_2$, where $\xi_2, \eta_2 \subset \mathfrak{J}_2^*$ and

$$v_{B_1}(\xi) > v_{B_1}(\xi_1) > 0, \qquad v_{B_1}(\xi_1) > v_{B_1}(\xi_2),$$
$$v_{B_1}(\eta) > v_{B_1}(\eta_1) > 0, \qquad v_{B_1}(\eta_1) > v_{B_1}(\eta_2).$$

More generally, if we assume that $B_1$ is of second kind with respect to $\mathfrak{J}^*$, $\mathfrak{J}_1^*, \mathfrak{J}_2^*, \cdots, \mathfrak{J}_m^*$, then we can find elements $\xi_i, \eta_i$ in each $\mathfrak{J}_i$ $(i = 1, 2, \cdots, m)$ such that $\alpha = \xi_i/\eta_i$ and

$$v_{B_1}(\xi) > v_{B_1}(\xi_1) > \cdots > v_{B_1}(\xi_m) > 0$$
$$v_{B_1}(\eta) > v_{B_1}(\eta_1) > \cdots > v_{B_1}(\eta_m) > 0.$$

Since the value group of $B_1$ is the group of integers, it follows that *$m$ cannot be greater than* $\min(v(\xi), v(\eta))$. Hence, for all $i$ sufficiently high, $B_1$ must be of first kind with respect to $\mathfrak{J}_i^*$, which proves our assertion.

We next show that $\Omega$ is a *proper subring* of $\Sigma$. In fact, let $\alpha, \beta$ be elements of $\mathfrak{J}^*$ such that $\alpha \not\equiv 0(\mathfrak{p}^*)$, $\beta \equiv 0(\mathfrak{p}^*)$. By the nature of the transformation

which carries from $\mathfrak{J}^*$ to $\mathfrak{J}_1^*$, we have that $\alpha/\beta$ is not in $\mathfrak{J}_1^*$. Moreover $\alpha \not\equiv 0(\mathfrak{p}_1^*)$, $\beta \equiv 0(\mathfrak{p}_1^*)$, whence $\alpha/\beta$ is not in $\mathfrak{J}_2^*$. More generally, $\alpha/\beta \notin \mathfrak{J}_i^*$, for all $i$, i.e. $\alpha/\beta \notin \Omega$.

On the basis of these results, theorem 10 now appears as a special case of the following general

LEMMA. *Let*

$$\mathfrak{J}^* \subset \mathfrak{J}_1^* \subset \cdots \subset \mathfrak{J}_i^* \subset \cdots$$

*be an arbitrary (non necessarily normal) infinite ascending sequence of integrally closed quotient rings: $\mathfrak{J}_i^* = Q(P_i)$, and let $\Omega = \lim \mathfrak{J}_i^*$. If $\Omega$ is a proper subring of $\Sigma$, and if every one-dimensional valuation $B_1$ of $\Sigma$, whose valuation ring contains $\Omega$, is necessarily of the first kind with respect to some $\mathfrak{J}_i^*$ (and hence also with respect to all $\mathfrak{J}_j^*$, $j \geqq i$), then $\Omega$ is the valuation ring of a zero-dimensional valuation.*[23]

PROOF OF THE LEMMA. The proper subring $\Omega$ of $\Sigma$ is integrally closed, and is therefore, at any rate, the intersection of the valuation rings containing it. We assert, that in the representation of $\Omega$ as an intersection of valuation rings, it is permissible to omit all the rings which belong to one-dimensional valuations. To prove this assertion, it is sufficient to show that if $B_1$ is a one-dimensional valuation, whose ring $\mathfrak{B}_1$ contains $\Omega$, then $\Omega$ is already contained in the valuation ring $\mathfrak{B}_0$ of a zero-dimensional valuation, such that $\mathfrak{B}_0 \subset \mathfrak{B}_1$. The valuation $B_1$ maps $\Sigma$ upon a field $\Sigma^*$ of algebraic functions of one variable. By hypothesis, for some $i = m$, it will be true that $B_1$ is of first kind with respect to all $\mathfrak{J}_i^*$ $i \geqq m$. The prime ideal of $B_1$ in $\mathfrak{J}_i^*$ is then one dimensional, say $\bar{\mathfrak{p}}_i$. We consider the ring of residual classes $R_i^* = \mathfrak{J}_i^*/\bar{\mathfrak{p}}_i$. $R_i^*$ is a subring of $\Sigma^*$, and $\Sigma^*$ is the quotient field of $R_i^*$, since $\mathfrak{J}_i^*$ is integrally closed in $\Sigma$. Moreover, $R_i^*$ is the quotient ring of a prime ideal of a finite integral domain in $\Sigma^*$, because the same is true of $\mathfrak{J}_i^*$ in the field $\Sigma$. Hence *$R_i^*$ is contained in at least one and in at most a finite set of valuation rings of $\Sigma^*$*. Let $H_i$ be the (finite and non-vacuous) set of "places" (prime divisors) of $\Sigma^*$ whose valuation rings contain $R_i^*$. Since $\bar{\mathfrak{p}}_i = \bar{\mathfrak{p}}_{i+1} \cap \mathfrak{J}_i^*$, it follows that $R_i^* \subseteq R_{i+1}^*$, whence *$H_{i+1}$ is a subset of $H_i$*. Since no $H_i$ is vacuous and each $H_i$ consists of a finite number of places, it follows that at least one "place" $\mathfrak{P}$ of $\Sigma^*$ belongs to all sets $H_i$. This place $\mathfrak{P}$ of $\Sigma^*$ determines a zero-dimensional valuation $B$ of $\Sigma$, composed with

[23] The following is an example in which the last condition of the lemma is not satisfied. Let $\Sigma = \mathsf{K}(x, y)$, $\mathfrak{o} = \mathsf{K}[x, y]$, $\mathfrak{o}_i = \mathsf{K}[x, y, y^2/x, \cdots, y^i/x^{i-1}]$. Each ring $\mathfrak{o}_i$ is integrally closed in $\Sigma$ and $\mathfrak{o}_i \cdot (x, y, y^2/x, \cdots, y^i/x^{i-1})$ is a prime zero-dimensional ideal $\mathfrak{p}_i$ in $\mathfrak{o}_i$. Let $\mathfrak{J}_i^* = \mathfrak{o}_i\mathfrak{p}_i$. The quotient rings $\mathfrak{J}^*, \mathfrak{J}_1^*, \cdots$ are all integrally closed and form a strictly ascending sequence. If we put $x' = x$, $y' = \frac{y}{x}$, then $\mathfrak{o}_i = \mathsf{K}[x', x'y', \cdots, x'y'^i]$, and hence the one-dimensional valuation defined by the prime ideal $(x')$ in the ring $\mathsf{K}[x', y']$ is of second kind with respect to each $\mathfrak{J}_i^*$. The elements $\frac{y}{x}$ and $\frac{x}{y}$ do not belong to any of the rings $\mathfrak{J}_i^*$, and hence the union of the rings $\mathfrak{J}_i^*$ is not a valuation ring.

$B_1$, and clearly the valuation ring of $B$ contains each quotient ring $Q(P_i)$ and is contained in $\mathfrak{B}_1$, q.e.d.

We may then assert that $\Omega$ is the intersection of valuation rings belonging to zero-dimensional valuations. Hence, in order to prove our lemma, we have only to prove that $\Omega$ *is not contained in two distinct zero-dimensional valuation rings.*

Let us assume that there exist two distinct zero-dimensional valuations $B$ and $B'$ whose valuations rings contain $\Omega$. Let $F_1$ be a projective model (for instance, a normal model) of the field on which the centers of $B$ and $B'$ are two *distinct* points, say $A$ and $A'$ (the existence of such a surface $F_1$ follows quite trivially from the hypothesis that $B$ and $B'$ are distinct valuations). Let moreover, $F^{(i)}$ be some projective model of $\Sigma$ (for instance, a normal model) such that $\mathfrak{J}_i^*$ is the quotient ring of a point $P_i$ on $F^{(i)}$. Since the valuation ring of $B$ contains $\Omega$, its center on $F^{(i)}$ is the point $P_i$. Hence $P_i$ and $A$ are corresponding points in the birational correspondence between $F_1$ and $F^{(i)}$. Similarly, $P_i$ and $A'$ are corresponding points. Since to $P_i$ there thus correspond two distinct points of $F_1$ and since $Q(P_i)$ is integrally closed, it follows, by theorem 5, that $P_i$ must be a fundamental point. Let $\Gamma_i$ be the set of fundamental curves on $F_1$ which correspond to $P_i$. Let $\Gamma_{i+1,j}$ be an irreducible component of $\Gamma_{i+1}$. There exists a one-dimensional valuation whose center on $F_1$ is $\Gamma_{i+1,j}$ and whose center on $F^{(i+1)}$ is $P_{i+1}$. The center of this valuation on $F^{(i)}$ will then be $P_i$, since $Q(P_i) \subset Q(P_{i+1})$. Hence $\Gamma_{i+1,j}$ is also a fundamental curve for $P_i$ and for the birational correspondence between $F^{(i)}$ and $F_1$. Thus, *every irreducible component* of $\Gamma_{i+1}$ *is also a component of* $\Gamma_i$. Since the number of irreducible components in a $\Gamma_i$ is finite, and $> 1$, it follows that *there exists an irreducible curve* $\Gamma$ *on* $F_1$, *which belongs to each curve* $\Gamma_{i+1}$. There exists therefore a 1-dimensional valuation (whose center on $F_1$ is the curve $\Gamma$) which is of second kind with respect to each ring $Q(P_i)$, in contradiction with our hypothesis. This proves our lemma and theorem 10.

## 20

"Local Reduction" Theorem: *If* $\mathfrak{J}^* = Q(P)$, $\mathfrak{J}_1^* = Q(P_1)$, $\cdots$ *is a normal sequence of quotient rings, then, for some integer* $m$, *all points* $P_i$, $i \geqq m$, *are simple points.*

Proof. Let $\Omega = \operatorname{Lim} \mathfrak{J}_i^*$, and let $B$ be the zero-dimensional valuation whose valuation ring $\mathfrak{B}$ coincides with $\Omega$ (by theorem 10). We apply our fundamental lemma (proved in Part II). There exist, according to this lemma, a projective model of $\Sigma$ on which the center of $B$ is a simple point $A$. We consider the quotient ring $\mathfrak{o}^* = Q(A)$. It is contained in $\mathfrak{B}$, whence the valuation $B$ determines in $Q(A)$ a tangential ideal $\mathfrak{q}^*$ (V, 18). The ideal $\mathfrak{q}^*$ determines a quotient ring $\mathfrak{o}' = Q(A')$, obtainable from $Q(A)$ by a quadratic transformation and evidently contained in $\mathfrak{B}$. The prime zero-dimensional ideal of $\mathfrak{o}'$ splits, in the integral closure $\bar{\mathfrak{o}}'$ of $\mathfrak{o}'$, into a finite number of prime zero-dimensional ideals, one of which, say $\mathfrak{p}$, will be the contracted ideal of the

ideal of non-units in $\mathfrak{B}$. We pass to the quotient ring $\mathfrak{o}_1^* = \mathfrak{o}_1' = Q(A_1)$. This ring is obtained from $\mathfrak{o}^*$ by a quadratic transformation, followed by integral closure. Continuing this process, we get a normal sequence

$$\mathfrak{o}^* = Q(A), \quad \mathfrak{o}_1^* = Q(A_1), \quad \mathfrak{o}_2^* = Q(A_2), \cdots .$$

The quotient rings $\mathfrak{o}_i^*$ are all contained in $\mathfrak{B}$. Hence, by theorem 10, Lim $\mathfrak{o}_i^* =$ Lim $\mathfrak{J}_i^* = \mathfrak{B}$.

Let $x$, $y$ be uniformizing parameters at the simple point $A$, which we may assume to be the point $x = y = z = 0$ on some surface $f(x, y, z) = 0$. The elements of $\mathfrak{o}^*$ are those elements of $\Sigma$ which are formal power series in $x$ and $y$. We may assume $v(y) > v(x)$, and also $v(z) > v(x)$. Our quadratic transformation with fundamental point at $A$ consists then in passing from the ring $\mathsf{K}[x, y, z]$ to the ring $\mathsf{K}[x_1, y_1, z_1]$, where $x_1 = x$, $y_1 = y/x$, $z_1 = z/x$, and the point $A'$ is the point $x' = y' = z' = 0$. This point is clearly a simple point of the transformed surface $f_1(x_1, y_1, z_1) = 0$, since $z_1 = 0$ is a simple root of $f_1(0, 0, z_1)$. Hence $Q(A')$ itself is already integrally closed; $Q(A') = Q(A_1)$ and $Q(A_1)$ consists of all elements of $\Sigma$ which are holomorphic functions of the new elements $x_1$, $y_1$. In conclusion, the passage from $Q(A)$ to $Q(A_1)$ is simply effected by a quadratic transformation applied to the uniformizing variables. The points $A_i$ are all simple points.

We shall denote by $x_i$, $y_i$ the uniformizing parameters at $A_i$. Following the notations of IV, 15, we denote the prime zero-dimensional ideals of $\mathfrak{J}^*$ and $\mathfrak{o}^*$ by $\mathfrak{P}_0$, $\mathfrak{p}_0$ respectively. The prime zero-dimensional ideals of $\mathfrak{J}_i^*$ and $\mathfrak{o}_i^*$ will be denoted by $\mathfrak{P}_i$ and $\mathfrak{p}_i$ respectively.

Since the rings $\mathfrak{J}_i^*$ and $\mathfrak{o}_i^*$ have the same limit ring, namely $\mathfrak{B}$, and since each of the rings $\mathfrak{J}_i^*$, $\mathfrak{o}_i^*$ is a quotient ring in a finite integral domain, it follows that each $\mathfrak{J}_i^*$ is a subring of some $\mathfrak{o}_j^*$, and each $\mathfrak{o}_i^*$ is a subring of some $\mathfrak{J}_j^*$. Dropping, if necessary, a finite number of elements in the normal sequence $\{\mathfrak{J}_i^*\}$, we may assume that already the first ring, $\mathfrak{J}^*$, contains the ring $\mathfrak{o}^*$. If $\mathfrak{J}^*$ also contains $\mathfrak{o}_1^*, \cdots, \mathfrak{o}_m^*$, but does not contain $\mathfrak{o}_{m+1}^*$, we may start with $\mathfrak{o}_m^*$ as the first member of the sequence $\{\mathfrak{o}_i^*\}$. Hence we may assume that $\mathfrak{J}^* \supseteq \mathfrak{o}^*$, $\mathfrak{J}^* \not\supseteq \mathfrak{o}_1^*$.

If $\mathfrak{J}^* = \mathfrak{o}^*$, there is nothing to prove: $P$ is then a simple point. Assume then that $\mathfrak{o}^*$ *is a proper subring of* $\mathfrak{J}^*$. We can apply Theorem 8. According to that theorem, the elements of $\mathfrak{J}^*$ are all of the form $\alpha/\beta$, where $\alpha, \beta \subset \mathfrak{o}^*$, $\alpha, \beta \equiv 0(\mathfrak{A}^\sigma)$, $\beta \not\equiv 0(\mathfrak{A}^{\sigma-1}\mathfrak{a})$, $\sigma$—an integer. We now make use of theorem 9. The hypothesis of that theorem was that $\mathfrak{a}$ is exactly divisible by $\mathfrak{p}_0^{e+1}$, if $\mathfrak{A}$ is exactly divisible by $\mathfrak{p}_0^e$. We show that this hypothesis is satisfied in the present case and that it is a consequence of our assumption $\mathfrak{J}^* \not\supseteq \mathfrak{o}_1^*$. In fact, let us assume that $\mathfrak{a}$ is not divisible by $\mathfrak{p}^{e+1}$, whence $\mathfrak{a}$ is exactly divisible by $\mathfrak{p}^e$. We consider the decomposition of $\mathfrak{A}$ and $\mathfrak{a}$ into simple $v$-factors. We make use of the fact that the system of subforms of a simple $v$-ideal $\mathfrak{P}$, of kind $> 1$, is of dimension zero (see $Z_1$, p. 163, Corollary 3.2). According to this result, there is associated with every simple $v$-ideal $\mathfrak{P}$, of kind $> 1$, a linear form $ax + by$.

If $\mathfrak{P}$ is exactly divisible by $\mathfrak{p}_0^m$, then every element in $\mathfrak{P}$ is of the form: $c\cdot(ax+by)^m$ + terms of higher degree. Let $a_ix+b_iy$, $i=1,2,\cdots,s$, be the *distinct* linear forms associated with the various simple $v$-factors of $\mathfrak{A}$ and $\mathfrak{a}$, We include among these forms also the form $y$, although *a priori* there may be no simple $v$-factor associated with $y$. Let, say, $a_1x+b_1y=y$ (i.e. $a_1=0$. $b_1=1$). We can then write the ideals $\mathfrak{A}$ and $\mathfrak{a}$ in the form:

$$\mathfrak{A}=\mathfrak{p}_0^m\mathfrak{A}_1\mathfrak{A}_2\cdots\mathfrak{A}_s,$$

$$\mathfrak{a}=\mathfrak{p}_0^n\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_s,$$

where $\mathfrak{A}_i$ is the product of the simple $v$-factors of $\mathfrak{A}$ associated with the form $a_ix+b_iy$. Similarly for $\mathfrak{a}_i$ and $\mathfrak{a}$. If no simple $v$-factor of $\mathfrak{A}$ is associated with $a_ix+b_iy$, then we put $\mathfrak{A}_i=(1)$. Similarly for $\mathfrak{a}$ and $\mathfrak{a}_i$.

For a given $i$ we consider the quadratic transformation $x'=x$, $y'=\dfrac{a_ix+b_iy}{x}$ (or $y'=y$, $x'=\dfrac{a_ix+b_iy}{y}$, if $b_i=0$) and we pass to the ring $\Omega'$ of formal power series of $x'$ and $y'$. Let $\mathfrak{A}_j$ be exactly divisible by $\mathfrak{p}_0^{m_j}$, and similarly, let $\mathfrak{a}_j$ be exactly divisible by $\mathfrak{p}_0^{n_j}$. It is clear that if $j\neq i$, then the transform of $\mathfrak{A}_j$ by our quadratic transformation is the unit ideal, i.e. $\Omega'\cdot\mathfrak{A}_j=(x'^{m_j})$. Similarly for $\mathfrak{a}_j$. On the other hand, since $\mathfrak{a}\equiv 0(\mathfrak{A})$, also $\Omega'\cdot\mathfrak{a}\equiv 0(\Omega'\cdot\mathfrak{A})$. Hence the transform of $\mathfrak{a}_i$ must be a multiple of, or coincide with the transform of $\mathfrak{A}_i$. This implies that $\mathfrak{a}_i$ itself is a multiple of $\mathfrak{A}_i$ (see $Z_1$, section 12). We have therefore $\mathfrak{a}_i=0(\mathfrak{A}_i)$, for $i=1,2,\cdots,s$. Now $\mathfrak{a}$ is a maximal subideal of $\mathfrak{A}$. Hence at most one of the ideals $\mathfrak{a}_i$ can be a proper multiple of the corresponding ideal $\mathfrak{A}_i$.[24] We show that $\mathfrak{a}_1$ is necessarily a proper subideal of $\mathfrak{A}_1$. Namely, assume that $\mathfrak{a}_1=\mathfrak{A}_1$. Since in our valuation $B$ we have $v(y)>v(x)$, and since the coefficient $b_i$ in the form $a_ix+b_iy$ is different from zero if $i\neq 1$, it follows that $v(\mathfrak{A}_i)=v(\mathfrak{p}_0^{m_i})$, $i\neq 1$. Similarly, $v(\mathfrak{a}_i)=v(\mathfrak{p}_0^{n_i})$, if $i\neq 1$. Hence, if $\mathfrak{a}_1=\mathfrak{A}_1$, then $v(\mathfrak{A})=v(\mathfrak{a})$, since $m+m_1+\cdots+m_s=n+n_1+\cdots+n_s=\rho$ (see also preceding footnote). This is in contradiction with the definition of the ideals $\mathfrak{A}$ and $\mathfrak{a}$.

We have then $\mathfrak{A}_1\neq\mathfrak{a}_1$, $\mathfrak{A}_i=\mathfrak{a}_i$, $i=2,\cdots,s$. Now consider any valuation $B'$ of center $P$. We must have $v_{B'}(\mathfrak{A})<v_{B'}(\mathfrak{a})$. Hence $v_{B'}(\mathfrak{A}_1)<v_{B'}(\mathfrak{a}_1)$, or $v_{B'}(\mathfrak{A}_1\mathfrak{p}_0)<v_{B'}(\mathfrak{a}_1)$, according as $m=n$, or $m=n+1$ (see preceding footnote). Since the subform of $\mathfrak{a}_1$ is $y^{n_1}$, it follows that necessarily $v_{B'}(y)>v_{B'}(x)$. Since

[24] *Proof.* We observe that the dimension $s$ of the subforms (of degree $\rho$) of $\mathfrak{A}$ is $m$, since $\mathfrak{A}$ has the factor $\mathfrak{p}_0^m$. Similarly, the dimension of the subforms of $\mathfrak{a}$ is $n$. Since $\mathfrak{a}$ is a maximal subideal of $\mathfrak{A}$, necessarily $n$ is either $m$ or $m-1$. If $n=m$, the assertion in the text is trivial. Suppose that $n=m-1$. Since $m+m_1+\cdots+m_s=n+n_1+\cdots+n_s$ and $n_j\geqq m_j$, for all $j$, we deduce that $n_i=m_i+1$, for some $i$, while $n_j=m_j$, $j\neq i$. Hence $\mathfrak{a}_i\neq\mathfrak{A}_i$ and therefore $\mathfrak{a}_i$ is a proper multiple of $\mathfrak{A}_i$. Since $\mathfrak{a}_i$ is exactly divisible by $\mathfrak{p}_0^{m_i+1}$, while $\mathfrak{A}_i$ is exactly divisible by $m_i$, it follows ($Z_1$, section 12), that $\mathfrak{a}_i$ is also a multiple of $\mathfrak{p}_0\mathfrak{A}_i$. Hence the ideal $\mathfrak{p}_0^n\mathfrak{A}_1\cdots\mathfrak{A}_{i-1}\mathfrak{a}_i\mathfrak{A}_{i+1}\cdots\mathfrak{a}_s$ is a proper multiple of $\mathfrak{A}$ and divides $\mathfrak{a}$. Consequently it coincides with $\mathfrak{a}$, q.e.d.

this is true for any zero-dimensional valuation of center $P$, it follows that the uniformizing parameters $x_1 = x$, $y_1 = y/x$ for the point $A_1$ are in $Q(P)$. Hence $Q(A_1) \subseteq Q(P)$, and this proves our assertion.

In view of theorem 9 we can therefore assert that the simple $v$-factors of $\mathfrak{a}$ are predecessors of, or coincide with, the simple $v$-factors of $\mathfrak{A}$. Let $\mathfrak{o}_h^*$ be the first ring in the sequence $\{\mathfrak{o}_i^*\}$ such that $\mathfrak{o}_h^* \supseteq \mathfrak{J}^*$ (such a ring exists, since $\operatorname{Lim} \mathfrak{o}_i^* = \mathfrak{B}$). By theorem 8, the elements of $\mathfrak{J}^*$ are all of the form $\alpha/\beta$, where $\alpha, \beta \equiv 0(\mathfrak{A}^\sigma)$, $\beta \not\equiv 0(\mathfrak{A}^{\sigma-1}\mathfrak{a})$, $\sigma$—an arbitrary integer. All such quotients $\alpha/\beta$ must be therefore elements of $\mathfrak{o}_h^*$. But this is only possible if and only if the transform of the ideal $\mathfrak{A}$ by the sequence of quadratic transformations, carrying $\mathfrak{o}^*$ into $\mathfrak{o}_h^*$, is the unit ideal. In other words, the extended ideal $\mathfrak{o}_h^*\mathfrak{A}$ must be a principal ideal in $\mathfrak{o}_h^*$:

$$\mathfrak{o}_h^*\mathfrak{A} = \mathfrak{o}_h^* \cdot \xi^{(h)}.$$

Moreover, $h$ must be the lowest integer for which this reduction of $\mathfrak{A}$ to the unit ideal takes place. Or, to be quite explicit: if $\mathfrak{A} = \mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_\mu^{\alpha_\mu}$ and if $P_i$ is a simple $v$-ideal of kind $h_i$, then $h = \text{maximum } (h_1, \cdots, h_\mu)$. By theorem 9, the reduction of the ideal $\mathfrak{a}$ to the unit ideal will also take place at this stage, or even perhaps earlier, (i.e. in some ring $\mathfrak{o}_i^*$, $i < h$). Now, the prime ideal $\mathfrak{P}_0$ of $\mathfrak{J}^*$ consists of all those quotients $\alpha/\beta$ in which $\alpha \equiv 0(\mathfrak{A}^{\rho-1}\mathfrak{a})$. Hence —*and this is the goal we were aiming for*—we can state the following

LEMMA. *The extended ideal $\mathfrak{o}_h^*\mathfrak{P}_0$ is a principal ideal.*

On the basis of this lemma the proof of the local reduction theorem is rapidly completed. Let

$$\mathfrak{o}_h^*\mathfrak{P}_0 = \mathfrak{o}_h^* \cdot \alpha_h, \qquad \alpha_h \subset \mathfrak{o}_h^*. \tag{36}$$

Let $\mathfrak{Q}^*$ be the tangential ideal of $\mathfrak{J}^*$ (relative the valuation $B$ whose valuation ring is the limit of the rings $\mathfrak{J}_i^*$). We have then

$$v_B(\mathfrak{Q}^*) > v_B(\mathfrak{P}_0). \tag{37}$$

By (36), every element $\eta$ of $\mathfrak{P}_0$ is of the form: $\eta = \xi \cdot \alpha_h$, $\xi \subset \mathfrak{o}_h^*$. By (37), $\eta$ is an element of $\mathfrak{Q}^*$ *if and only if $\xi$ is not a unit in* $\mathfrak{o}_h^*$. It follows that the intermediate quotient ring $\mathfrak{J}'$, between $\mathfrak{J}^*$ and $\mathfrak{J}_1^*$, obtained from $\mathfrak{J}$ by a quadratic transformation, is contained in $\mathfrak{o}_h^*$. Since $\mathfrak{J}_1^*$ is obtained from $\mathfrak{J}'$ by a process of integral closure and since $\mathfrak{o}_h^*$ is integrally closed, it follows that the *entire ring $\mathfrak{J}_1^*$ is contained in* $\mathfrak{o}_h^*$.

Let us review in a few words the essence of the preceding results. We have focused our attention on the last ring of the sequence $\{\mathfrak{o}_i^*\}$ which is contained in $\mathfrak{J}^*$. For simplicity we took that ring as the first ring $\mathfrak{o}^*$ of the sequence. We had then $\mathfrak{J}^* \supseteq \mathfrak{o}^*$, $\mathfrak{J}^* \not\supseteq \mathfrak{o}_1^*$. We have assumed that $\mathfrak{o}^*$ is a proper subring of $\mathfrak{J}^*$, and on the basis of this assumption we have proved that, if $\mathfrak{o}_h^*$ is the first ring $\mathfrak{o}_i^*$ such that $\mathfrak{J}^* \subseteq \mathfrak{o}_i^*$, then $\mathfrak{o}_h^*\mathfrak{P}_0$ is a principal ideal. From this alone we have concluded that also $\mathfrak{J}_1^* \subseteq \mathfrak{o}_h^*$. Hence we can assert the following: *if $\mathfrak{o}_h^*$ is the first ring in the sequence $\{\mathfrak{o}_i^*\}$ which contains $\mathfrak{J}^*$ and if $\mathfrak{J}^* \neq \mathfrak{o}_h^*$, then*

$\mathfrak{o}_h^*$ *also contains* $\mathfrak{J}_1^*$. Obviously, $\mathfrak{o}_h^*$ is also the first ring $\mathfrak{o}_i^*$ which contains $\mathfrak{J}_1^*$. Hence if $\mathfrak{J}_1^*$ does not coincide with $\mathfrak{o}_h^*$, we conclude that $\mathfrak{o}_h^*$ contains $\mathfrak{J}_2^*$, and so on. Since the limit of the rings $\mathfrak{J}_i^*$ is the entire valuation $\mathfrak{B}$ of $B$, it follows that for some integer $m$ we must have $\mathfrak{J}_m^* = \mathfrak{o}_h^*$. The point $P_m$, and every point $P_i$, $i \geqq m$, is then necessarily a simple point, q.e.d.

## VI. Reduction of the Singularities

### 21

We start with a *normal* projective model $F$ of our field $\Sigma$ in a projective space $P_m(y_0, \cdots, y_m)$. Let $\omega_0, \omega_1, \cdots, \omega_m$ be the homogeneous coördinates of the general point of $F$. The surface $F$ has at most a finite number of singular points. Let $P$ be one of them. Without loss of generality we may assume that $P$ is the point $y_0 = 1$, $y_1 = \cdots = y_m = 0$. We apply the quadratic transformation (28) of V, 18 and we get the transformed surface $F'$. The birational correspondence between $F$ and $F'$ has been studied in Part V and its properties were reassumed at the end of section 18. The surface $F'$ may not be normal in its ambient projective space. If it is not normal, we apply to $F'$ the birational transformation of integral closure described in the introduction, getting a new well-defined normal projective model $F_1$ of our field $\Sigma$. The resulting correspondence between the points of $F$ and $F_1$ is again one to one, with the exception of the point $P$. In fact, if $A$ is a point of $F$ different from $P$, and if $A'$ is the corresponding points of $F'$, then we know that $Q(A) = Q(A')$. Since $F$ is normal, $Q(A)$ is integrally closed in $\Sigma$. Hence also $Q(A')$ is integrally closed in $\Sigma$, and consequently, *$A'$ goes into a unique point $A_1$ of $F_1$, and there is invariance of quotient rings*:

$$Q(A_1) = Q(A') = Q(A).$$

The points $P_1$ of $F_1$ which correspond to the fundamental point $P$ on $F$ are those which correspond to the points $P'$ on the fundamental curve $\Gamma$ on $F'$. The relation between $Q(P)$ and $Q(P_1)$ is clearly the outcome of two operations:

($\alpha$) *the quotient formation in terms of a tangential ideal in* $Q(P)$; this yields $Q(P')$;

($\bar{\alpha}$) *the splitting of the prime zero-dimensional ideal of* $Q(P')$ *into primary factors* $\bar{\mathfrak{q}}_i$ *in the integral closure* $\overline{Q(P')}$ of $Q(P')$; the quotient ring $Q(P_1)$ is the quotient ring of one of the corresponding prime ideals $\bar{\mathfrak{p}}_i$. These operations are exactly those described in section 19: a quadratic transformation followed by integral closure.

*If $A$ is a simple point of $F$, the corresponding point $A_1$ of $F_1$ is also a simple point.* This follows from the invariance of quotient rings and from the fact, pointed out in the introduction, that the property of being a simple point is entirely a property of the quotient ring of that point. Since $F_1$ is normal, it has at most a finite number of singular points. Among these, there are in the first place those which correspond to the singular points of $F$, different from $P$—

and here we have no change in the quotient rings of corresponding points. The remaining singular points of $F_1$ correspond to $P$, and their quotient rings are obtained from $Q(P)$ by a quadratic transformation followed by integral closure. Thus *$P$ has been resolved into a finite number of singular points $P_1$ whose quotient rings are more inclusive than $Q(P)$.*

If $F_1$ still has singular points, we take one of them, say $P_1$, as fundamental point of a quadratic transformation, getting a new surface $F_1'$. From $F_1'$ we pass to the corresponding normal surface $F_2$. We repeat this process indefinitely, getting a *sequence of normal surfaces*:

$$F, F_1, F_2, \cdots. \tag{38}$$

We now prove our main theorem:

THEOREM OF REDUCTION OF SINGULARITIES: *After a finite number of quadratic and integral closure transformations, a normal surface $F_i$ is obtained which is free from singularities.*

This main theorem is an immediate consequence of the "local reduction" theorem proved in part V. We consider the set $M$ of all *normal* sequences $\{Q(P), Q(P_1), \cdots\}$ where the first point $P$ is a *fixed* point of the given surface $F$. For each such sequence, let $h$ be the smallest possible value of $i$ such that $P_i$ is a simple point. Then of course also all $P_i$, $i > h$, are simple points. The integer $h$ depends on the sequence. We show however that *as the sequence $\{Q(P_i)\}$ varies in $M$, the integer $h$ has a finite upper bound.* In fact, assuming the contrary, there would exist, *for any integer $\nu$*, a sequence

$$\{Q(P_i^{\nu})\}: Q(P), Q(P_1^{(\nu)}), Q(P_2^{(\nu)}), \cdots, Q(P_i^{(\nu)}), \cdots$$

such that $P_1^{(\nu)}, \cdots, P_\nu^{(\nu)}$ are singular points (on their respective surfaces). Now the points $P_1^{(\nu)}$ can all be realized on the surface $F_1$ of the sequence (38) of normal surfaces. They are namely the points which correspond to the point $P$ of $F$. Since $F_1$ has only a finite number of singular points, one and the same point, say $P_1$, must occur in infinitely many of the sequences $\{Q(P_i^{(\nu)})\}$. If $F_2$ is the normal surface obtained from $F_1$ by taking $P_1$ as the fundamental point of the quadratic transformation, then the points $P_2^{(\nu)}$, belonging to the sequences $\{Q(P_i^{(\nu)})\}$ in which $P_1^{(\nu)} = P_1$, are points of $F_2$. Hence, by the same argument, there must exist infinitely many sequences $\{Q(P_i^{(\nu)})\}$ in which $P_1^{(\nu)} = P_1$ *and* $P_2^{(\nu)} = P_2$, where $P_2$ is a fixed point of $F_2$. Continuing in this fashion, we get an *infinite sequence* of points $P, P_1, P_2, \cdots$, all singular on their respective surfaces $F, F_1, F_2, \cdots$, and such that the sequence $\{Q(P_i)\}$ is normal. This is in contradiction with the "local reduction" theorem.

Let $g = g(P)$ be the least upper bound of $h$. The integer $g(P)$ is a numerical character of $P$. Clearly, *$P$ is a simple point if and only if $g(P) = 0$.* Let $P', \cdots, P^{(\rho)}$ be the singular points of $F$, and let $\gamma = \max(g(P'), g(P''), \cdots, g(P^{\rho}))$. Let $P', P'', \cdots, P^{(\rho)}$, $\rho \leqq \sigma$, be the points for which the character $g$ is exactly equal to $\gamma$. We choose $P'$ as fundamental point of our quadratic

transformation and we pass from $F$ to the normal surface $F_1$. If $P_1'$ is a singular point of $F_1$ which corresponds to $P'$, then it is obvious that $g(P_1') < g(P')$. If $P_1'', \cdots, P_1^{(\sigma)}$ are the points of $F_1$ which correspond to $P'', \cdots, P^{(\sigma)}$ respectively, then $g(P^{(j)}) = g(P_1^{(j)})$. Hence $F_1$ contains only $\rho - 1$ singular points for which the character $g$ equals $\gamma$, while for any other singular point of $F_1$ the character $g$ will be less than $\gamma$. If we repeat this procedure $\rho$ times, always taking as fundamental point on $F_i$ $(i = 1, \cdots \rho - 1)$ a singular point whose character $g$ is equal to $\gamma$, we will get a normal surface $F_\rho$ on which *the character $g$ for each singular point is less than $\gamma$*. Ultimately, after a finite number of steps, a surface $F_i$ will be obtained, in which every point is a simple point. This proves our main theorem.

THE JOHNS HOPKINS UNIVERSITY.

## REFERENCES


1. ALBANESE, G.: *Transformazione birazionale di una superficie algebrica qualunque in un'altra priva di punti multipli*, Rend. Circ. mat. Palermo, Vol. 48 (1924).
2. CHISINI, O.: *La risoluzione delle singolarità di una superficie mediante transformazioni birazionali dello spazio*, Mem. Accad. Sci. Bologna VII. s. Vol. 8 (1921).
3. JUNG, H. W. E.: *Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen $x$, $y$ in der Umgebung einer Stelle $x = a$, $y = b$.* J. reine angew. Math. Vol. 133 (1908).
4. KRULL, W. *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, IV, 3. This monograph is quoted as "K".
5. B. LEVI. *Sulla risoluzione delle singolarità puntuali delle superficie algebriche dello spazio ordinario per transformazioni quadratiche*, Ann. Mat. pura appl. II. s. Vol. 26 (1897).
6. B. LEVI. *Risoluzione delle singolarità puntuali delle superficie algebriche*, Atti Accad. Sci. Torino, Vol. 33 (1897).
7. SCHILLING, O. F. G.: *A generalization of local class field theory*, Am. J. of Math., vol. 60 (1938).
8. VAN DER WAERDEN, B.: *Moderne Algebra*, vol. II (second edition).
9. WALKER, R. J.: *Reduction of singularities of an algebraic surface*, Annals of Mathematics, Vol. 36 (1935).
10. ZARISKI, O.: *Polynomial ideals defined by infinitely near base points*, Am. J. of Math., Vol. 60 (1938) (quoted $Z_1$).
11. ZARISKI, O.: *Some results in the arithmetic theory of algebraic varieties*, Am. J. of Math.. Vol. 61 (1939) (quoted $Z_2$).

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# TRANSFORMATIONS OF FINITE PERIOD. II

BY P. A. SMITH

(Received February 24, 1939)

This paper is a continuation, and to some extent a completion of an earlier work (I) under the same title (these Annals, Vol. 39 (1938), pp. 127–164). In I we developed a theory of special homologies for a very general space $M$ subjected to a periodic homeomorphism $T$ with itself of prime period $p$, and made use of this theory in studying the nature of the set $L$ of fixed points under the hypothesis that $M$ possesses the same homology characters as an $n$-sphere. This enabled us to go far toward determining the nature of $L$ in the special case that $M$ is a Euclidean 3-sphere. In the present work we propose (1) to abandon all restrictions concerning the homology characters of $M$ in the large and to look for such *local* properties of regularity in $M$ as will be transmitted to $L$; (2) to complete the analysis of $L$ when $M$ is a 3-sphere; (3) to prove for a general case the fact referred to elsewhere[1] that the components of $L$ are orientable if $M$ is orientable and $p$ is odd; (4) to reduce as far as possible the restriction that $p$ be prime. With regard to (4) we have been able to show that nearly all our results hold equally well when the period of $T$ is a power of a prime. In some cases it has been possible to remove all restrictions on $p$. Thus for example the fixed-point sets for perfectly arbitrary periodic homeomorphisms of a 3-sphere with itself are now completely known (theorem 4).

**5.1.**[2] *Local properties of spaces.* Throughout this paper the word *space* will mean a bicompact Hausdorff space $M$ such that (1) every open set in $M$ is the sum of a denumerable family of closed sets; (2) the Menger-Urysohn dimension of $M$ is finite (cf. 2.13). The main results in dimension theory hold in any bicompact space which satisfies (1) (Čech [2]). Moreover, as a consequence of (1) every space $M$ is completely normal (see footnote 8, 3.38) and has therefore the following property: if $K$ and $L$ are closed sets in $M$ and $\mathfrak{U}$ is a covering of $M$ (i.e. a finite covering by open sets), there exists a refinement $\mathfrak{U}_1$ of $\mathfrak{U}$ such that every $\mathfrak{U}_1$-chain which is simultaneously in $K$ and $L$ is in $KL$ (Čech [5]). The existence of refinements of this type leads easily to the following useful theorems:

A. *Let $N_1, \cdots, N_q$ be closed sets in the space $M$ and let $\gamma$ be a cycle in $N_1N_2 \cdots N_q$. Suppose that for each $\mathfrak{U}$ in a complete system $\{\mathfrak{U}\}$ of coverings*

[1] P. A. Smith, *The topology of transformation groups* (Bull. Am. Math. Soc., 44 (1938), pp. 497–514), p. 506.

[2] Sections numbered 1.1 to 4.16 are contained in our earlier paper I. Symbols of the form [$n$] will refer to the bibliography at the end of I.

*of $M$, there exists a chain $X(\mathfrak{U})$ such that $X(\mathfrak{U}) \subset N_i$ $(i = 1, \cdots, q)$ and $\phi X(\mathfrak{U}) = \gamma(\mathfrak{U})$, $\phi$ being the boundary operator. Then $\gamma \sim 0$ in $N_1 N_2 \cdots N_q$.*

B. *Let $K$, $N$, $L$ be closed sets in $M$ such that $K \subset N$ and let $\gamma$ be a cycle* mod *$LK$ in $LN$. Suppose that for each covering $\mathfrak{U}$ is a complete system $\{\mathfrak{U}\}$ there exists a chain $\eta(\mathfrak{U})$ such that* (1) *$\phi\eta(\mathfrak{U}) = \gamma(\mathfrak{U})$* mod *$K$;* (2) *$\eta(\mathfrak{U}) \subset L$;* (3) *$\eta(\mathfrak{U}) \subset N$. Then $\gamma \sim$* mod *$LK$ in $LN$.*

**5.2.** *Properties $P$ and $Q$.* Let $M$ be a space, $d$ a point in $M$, $\mathfrak{f}$ a field, to serve as a coefficient field for cycles and homologies, and $m$ an integer $\geqq 0$. We shall say that $M$ possesses property $P$ (relative to $\mathfrak{f}$) at $d$ provided there exists a neighborhood $D(d)$ and an $m$-cycle ${}^d\Omega_m$ mod $M - D$ such that (1) for no non-null open subset $D'$ of $D$ is ${}^d\Omega_m \sim 0$ mod $M - D'$; (2) for every neighborhood $B(b)$ contained in $D$ there exists a neighborhood $B'(b) \subset B$ such that ${}^d\Omega_m$ constitutes a basis for $m$-cycles mod $M - B$ relative to homologies mod $M - B'$ while (3) every cycle mod $M - B$ of dimension $\neq m$ is $\sim 0$ mod $M - B'$. A neighborhood $D(d)$ and cycle ${}^d\Omega_m$ satisfying (1), (2), (3) will be said to form a *fundamental pair* $(D(d), {}^d\Omega_m)$ for the point $d$.[3] It is obvious that $M$ can not simultaneously possess properties $P_m$ and $P_k$ at $d$ if $k \neq m$. Moreover, it follows readily from dimension theory that $M$ can only possess the property $P_m$ at $d$ if $m \leqq \dim M$.

Suppose $M$ possesses the property $P_m$ at every point $d$, $m$ depending on $d$. We shall then say that $M$ is of *type* $P$. If in particular $m$ is constant over $M$, $M$ is of type $P_m$. $M$ cannot be of types $P_m$ and $P_k$ if $k \neq m$. Moreover, it is easy to see that if $M$ is of type $P_m$ then at every point $d$, the local Betti numbers (Čech [4]) of $M$ relative to $\mathfrak{f}$ are the same as those at points in an $m$-cell. This is also true of the Betti numbers *in* $d$ (Alexandroff [8]) when $M$ is metric. In the metric case, $\dim_{\mathfrak{f}} M = m$ where $\dim_{\mathfrak{f}}$ means the dimension relative to the field $\mathfrak{f}$ (Alexandroff [7], [8]).

**5.3.** *If $M$ is connected and possess the property $P_0$ at $d$, then $M = d$.*

PROOF. Suppose there exists a neighborhood $A$ of $d$ such that $M - A \neq 0$. Then since $M$ is connected, it is easy to see that every relative 0-cycle in $M$ is $\sim 0$ mod $M - A$ (see [1], pp. 168–9). Since this is impossible, we conclude that $d$ possesses no neighborhood other than $M$ and hence $M = d$.

**5.4.** *Let $M$ be a space of type $P$. If $M$ is connected, there exists an integer $m$ such that $M$ is of type $P_m$.*

PROOF. Since $M$ is bicompact there can be chosen a finite set of neighborhoods $D_1(d_1), \cdots, D_q(d_q)$, a set of integers $m_1, \cdots, m_q$ and a set of cycles ${}^1\Omega_{m_1}, \cdots, {}^q\Omega_{m_q}$ mod $M - D_1, \cdots, M - D_q$ respectively such that $M \subset D_1 + \cdots + D_q$ and such that for each $i$, $({}^i\Omega_{m_i}, D_i)$ is a fundamental pair for $d_i$.

[3] With regard to 0-cycles we retain the convention adopted in 3.22 that a $(0, \mathfrak{U})$-chain is an absolute $(0, \mathfrak{U})$-cycle if and only if the sum of its coefficients is 0. *Every* $(0, \mathfrak{U})$-chain however is to be regarded as $(0, \mathfrak{U})$-cycle mod $A$ if $A \neq 0$.

Suppose for the moment that $D_1D_2 \neq 0$. Then $m_1 = m_2$. For suppose $m_1 < m_2$. Let $b$ be a point in $D_1D_2$. Since $b \subset D_2$, there exists a $B^*(b) \subset D_1D_2$ such that ${}^1\Omega_{m_1} \sim 0 \bmod M - B^*$. But since $B^* \subset D_1$, this contradicts (1) in the definition of $P_m$ at $d$.—Assume now that $M$ is connected. Then for any two $D$'s, say $D_i$ and $D_j$, there exists a sequence of $D$'s with these two for end-elements and such that each $D$ in the sequence (except the last) intersects its successor. From this we can conclude that $m_1 = m_2 = \cdots = m_q = m$ (say). We now order to each point $d$ of $M$ an integer $i(d)$ such that $d \subset D_{i(d)}$. Let $D(d) = D_{i(d)}$ and let ${}^d\Omega_m = {}^{i(d)}\Omega_m$. Then it is clear that for each $d$ in $M$, $(D(d), {}^d\Omega_m)$ is a fundamental pair and since $m$ is independent of $d$, $M$ is of type $P_m$.

**5.5.** We now recall the definition of local connectedness with respect to homology (HLC). The space $M$ is HLC$^n$ at the point $a$ if for every neighborhood $A(a)$ there exists an $A'(a) \subset A$ such that every cycle of dimension $\leqq n$ in $A'$ is $\sim 0$ in $A$. To say that $M$ is HLC$^n$ means that it is so at every point.

*A space $M$ which is* HLC$^0$ *can have only a finite number of components.*

PROOF. It will be sufficient to show that if $M$ is HLC$^0$, it has only a finite number of quasi-components, for then the quasi-components are identical with the components. (See Hausdorff, *Grundzüge der Mengenlehre*, page 248). Suppose there are infinitely many quasi-components. Then it will be possible to choose a point $a_0$ in a quasi-component $M_0$ such that $a_0$ is a limit point of a set $\{a_1, a_2, \cdots\}$ of points contained respectively in quasi-components $M_1$, $M_2, \cdots$ which are distinct from each other and from $M_0$. Since $M$ is HLC$^0$ there exists a neighborhood $A(a_0)$ such that every 0-cycle in $A(a_0)$ is $\sim 0$. There exists at least one $k > 0$ such that $a_k \subset A$. Let $\{\mathfrak{U}\}$ be a complete system of coverings for $M$. From each $\mathfrak{U}$ choose definite vertices $U_0$ and $U_k$ containing $a_0$ and $a_k$ respectively, and let $\alpha = \{U_0 - U_k\}$. $\alpha$ is a 0-cycle in $A$ and is therefore $\sim 0$. But since $a_0$ and $a_k$ lie in distinct quasi-components, the 0-cycle in question cannot possibly be $\sim 0$. (See [1], pp. 168–9) and therefore there cannot be infinitely many quasi-components.

*If $M$ is* HLC$^n$ *($n \geqq 0$), each component of $M$ is* HLC$^n$. For if $M$ is HLC$^n$, it is HLC$^0$ and its components are finite in number. By using the fact that $M$ is normal (since it is bicompact) it is a then simple matter to show that each component is HLC$^n$.

**5.6.** We shall say that $M$ possesses the property $Q$ at the point $d$ if for every neighborhood $A(d)$ there exists an $A'(d)$ with the property that for every neighborhood $B(b) \subset A'$, there is a $B'(b) \subset B$ such that every cycle mod $M - A$ in $M - B$ is $\sim 0 \bmod M - A'$ in $M - B'$. If $M$ possesses the property $Q$ at every point then $M$ is of type $Q$. If $M$ is of type $P$ (or $P_m$) *and* $Q$, then $M$ is of type $PQ$ (or $P_mQ$).

*If $M$ is of type $PQ$ and has only a finite number of components, then each component is of type $P_rQ$, $r$ depending on the component.* For, it is easy to see that

each component must be of type $PQ$ and the truth of our assertion then follows from 5.4.

EXAMPLES. Every finite simplicial complex is HLC$^n$ for arbitrary $n$ and relative to an arbitrary field $\mathfrak{f}$.

Every $m$-dimensional locally euclidean space is HLC$^n$ and of type $P_mQ$ ($n$ and $\mathfrak{f}$ arbitrary). Every absolute $m$-dimensional manifold mod $p$, $p$ a prime (Lefschetz, *Topology*, p. 120), is of type $P_mQ$ relative to the field $\mathfrak{p}$ of integers reduced modulo $p$. Conversely, if $M$ is a finite simplicial complex and is of type $P_mQ$ relative to a given $\mathfrak{f}$, then $M$ is $m$-dimensional and if it is not a manifold, it is at least a "pseudo-manifold" or simple circuit (Lefschetz, *Topology*, p. 47). There is no difficulty involved in verifying these statements and we shall omit the details.

**6.0.** *Periodic transformations.* Let $T$ be a periodic homeomorphism of a space $M$ with itself of prime period $p$, and let $L$ be the totality of fixed points of $T$. We assume always that $L \neq 0$ unless otherwise stated. From now on we shall denote generically by $\mathfrak{U}$ the special coverings (2.16) of $M$ relative to $T$. It follows from 2.18 that $\{\mathfrak{U}\}$ is a complete system for $M$. If $\mathfrak{U}$ and $\mathfrak{U}_1$ are special coverings such that $\mathfrak{U}_1 \subset \mathfrak{U}$, a *projection* of $\mathfrak{U}_1$ into $\mathfrak{U}$ will always be understood to mean an *invariant* projection (2.19). Under such projections, $\mathfrak{U}_1$-cycles of a given type (3.11) are carried into $\mathfrak{U}$-cycles of the same type.

We shall assume from now on unless otherwise stated that the coefficient field relative to which cycles and homologies are defined is the field $\mathfrak{p}$ (5.6). As in 3.9 we shall denote by $\sigma$ and $\bar{\sigma}$ the operators $1 + T + \cdots + T^{p-1}$ and $1 - T$ respectively and shall agree that the symbols $\rho$, $\bar{\rho}$ may stand either for $\sigma$ and $\bar{\sigma}$ or for $\bar{\sigma}$ and $\sigma$ respectively. It will be well to recall here that since $\mathfrak{U}$-simplexes which are not in $L$ are of dimension $\leqq n$, where $n = \dim M$, a relation of the form $\Gamma_n(\mathfrak{U}) \sim 0 \bmod B$ implies that $\Gamma_n(\mathfrak{U}) = 0 \bmod B + L$ (see 3.31, remark 1).

A further word concerning certain basic definitions in I. Suppose that $A$ is an invariant set in $M$ (i.e. a set such that $TA = A$). A chain $X(\mathfrak{U})$ is of type $(\rho, A)$ provided there exists a chain $Y(\mathfrak{U})$ such that $X(\mathfrak{U}) = \rho Y(\mathfrak{U}) \bmod A$. Suppose $B$ is an invariant set containing $A$ and that $C(\mathfrak{U})$ is a cycle mod $A$ in $B$, of type $(\rho, A)$. This means of course that the chain $C(\mathfrak{U})$ is in $B$, is a cycle mod $A$, and is of type $(\rho, A)$. The relation

$$C(\mathfrak{U}) \simeq 0 \bmod A \text{ in } B, \tag{1}$$

called a *special* homology, means that there exists in $B$ a chain $X(\mathfrak{U})$ of same type as $C(\mathfrak{U})$ (i.e. of type $(\rho, A)$) such that $\phi X(\mathfrak{U}) = C(\mathfrak{U}) \bmod A$, $\phi$ being the boundary operator. Evidently (1) implies a relation of the form

$$\phi(\rho W(\mathfrak{U}) + Z(\mathfrak{U})) = C(\mathfrak{U}) + Z^0(\mathfrak{U}) \tag{2}$$

where $\rho W(\mathfrak{U}) + Z(\mathfrak{U}) \subset B$, $Z(\mathfrak{U}) \subset A$, $Z^0(\mathfrak{U}) \subset A$. *We may assume that* $W(\mathfrak{U}) \subset B$. For let $B \cap H(\mathfrak{U})$ denote the subchain of $H(\mathfrak{U})$ which consists

of those simplexes of $H(\mathfrak{U})$ which are in $B$, each taken with the coefficient which it has in $B$. Then of course

$$B \cap (\rho W(\mathfrak{U}) + Z(\mathfrak{U})) = \rho W(\mathfrak{U}) + Z(\mathfrak{U}).$$

The expression on the left equals $B \cap \rho W(\mathfrak{U}) + B \cap Z(\mathfrak{U})$. Moreover, since $B$ is invariant, $\rho(B \cap W(\mathfrak{U})) = B \cap \rho W(\mathfrak{U})$. Hence (2) holds if $W(\mathfrak{U})$ is replaced by $W'(\mathfrak{U}) = B \cap W(\mathfrak{U})$ and $Z(\mathfrak{U})$ by $Z'(\mathfrak{U}) = B \cap Z(\mathfrak{U})$. Obviously $W'(\mathfrak{U}) \subset B$, $\rho W'(\mathfrak{U}) + Z(\mathfrak{U}) \subset B$, and $Z'(\mathfrak{U})$, since it is a subchain of $Z(\mathfrak{U})$, is in $A$. Thus our assertion is proved, and as a consequence, (1) always implies a relation of the form

$$\phi\rho Y(\mathfrak{U}) = C(\mathfrak{U}) \bmod A$$

where $Y(\mathfrak{U}) \subset B$.

We have consistently used special homologies in such a way that the relation $C(\mathfrak{U}) \simeq 0 \bmod A$ implies that $C(\mathfrak{U})$ is of type $(\rho, A)$. If $A'$ is an invariant set containing $A$ and if $C(\mathfrak{U})$ is of type $(\rho, A)$ we also allow relations of the form $C(\mathfrak{U}) \simeq 0 \bmod A'$. This however is not an inconsistency; for $C(\mathfrak{U})$ is obviously of type $(\rho, A')$ if it is of type $(\rho, A)$.

The remarks above apply to (Čech) *cycles* as well as $\mathfrak{U}$-cycles. Let us merely recall that $\{C(\mathfrak{U})\} = C$ is a cycle mod $A$ in $B$ of type $(\rho, A)$ ($A$, $B$ invariant, $A \subset B$) if for each $\mathfrak{U}$, $C(\mathfrak{U})$ is a $\mathfrak{U}$-cycle mod $A$ in $B$ of type $(\rho, A)$ and if, whenever $\mathfrak{U}_1 \subset \mathfrak{U}$, and $\pi = \pi(\mathfrak{U}_1, \mathfrak{U})$, we have $\pi C(\mathfrak{U}_1) \simeq C(\mathfrak{U}) \bmod A$ in $B$.—The set $B$ will of course be specified only if it is $\neq M$. The word "cycle" moreover will be used to mean "$\mathfrak{U}$-cycle" when this is clearly implied by the context.

**6.1.** The following lemmas will facilitate our study of the local properties of $L$.

LEMMA 1. *Let $B$ be an invariant set, possibly null and let $\Gamma(\mathfrak{U})$ be a chain of type $(\rho, B + L)$. There exists a chain $\Gamma'(\mathfrak{U})$ of type $(\rho, B)$ such that $\Gamma'(\mathfrak{U}) = \Gamma(\mathfrak{U}) \bmod L$. If $\Gamma(\mathfrak{U})$ is a cycle mod $B + L$, then $\Gamma'(\mathfrak{U})$ is a cycle mod $B$ and if $\Gamma(\mathfrak{U}) \simeq 0 \bmod B + L$, then $\Gamma'(\mathfrak{U}) \simeq 0 \bmod B$.*

PROOF. We may write $\Gamma(\mathfrak{U}) = \rho Y(\mathfrak{U}) \bmod B + L$ (6.0). It is easy to see then that there exists a relation of the form

$$\Gamma(\mathfrak{U}) = \rho Y(\mathfrak{U}) + Z(\mathfrak{U}) + Z'(\mathfrak{U}) \tag{1}$$

where $Z(\mathfrak{U}) \subset B$, $Z'(\mathfrak{U}) \subset L$. Let $\Gamma'(\mathfrak{U}) = \rho Y(\mathfrak{U}) + Z(\mathfrak{U})$. Then $\Gamma'(\mathfrak{U}) = \Gamma(\mathfrak{U}) \bmod L$. Moreover, $\Gamma'(\mathfrak{U}) = \rho Y(\mathfrak{U}) \bmod B$ so that $\Gamma'(\mathfrak{U})$ is of type $(\rho, B)$. Suppose $\Gamma(\mathfrak{U})$ is a cycle mod $B + L$. Then $\phi\Gamma(\mathfrak{U}) = 0 \bmod B + L$, and from (1) it follows that $\rho\phi Y(\mathfrak{U}) = 0 \bmod B + L$. No simplex of $\rho\phi Y(\mathfrak{U})$ can be in $L$ (3.33) and therefore $\rho\phi Y(\mathfrak{U}) = 0 \bmod B$. Hence $\phi\Gamma'(\mathfrak{U}) = 0 \bmod B$. Finally, suppose $\Gamma(\mathfrak{U}) \simeq 0 \bmod B + L$. Then we may write

$$\Gamma(\mathfrak{U}) = \rho Y(\mathfrak{U}) + Z(\mathfrak{U}) + Z'(\mathfrak{U}) = \phi\rho X(\mathfrak{U}) \bmod B + L.$$

Since $Z(\mathfrak{U}) + Z'(\mathfrak{U}) \subset B + L$, we have

$$\rho Y(\mathfrak{U}) = \phi\rho X(\mathfrak{U}) \bmod B + L. \tag{2}$$

Since $(\rho Y(\mathfrak{U})) \cap L = (\rho\phi X(\mathfrak{U})) \cap L = 0$ (3.33), the relation (2) holds mod $B$ and since $\Gamma'(\mathfrak{U}) = \rho Y(\mathfrak{U}) + Z(\mathfrak{U}) = \rho Y(\mathfrak{U}) \bmod B$, we have $\Gamma'(\mathfrak{U}) = \phi\rho X(\mathfrak{U})$ mod $B$, that is, $\Gamma'(\mathfrak{U}) \simeq 0 \bmod B$.

LEMMA 2. *Let $A(a)$ be an invariant neighborhood of $a$, $a \subset L$, and let $\gamma_k(\mathfrak{U})$ be a chain in $L$ which is a cycle* mod $M - A$. *Let $X_{k+1}(\mathfrak{U})$ be a chain such that $\phi X(\mathfrak{U}) = \gamma(\mathfrak{U}) \bmod M - A$. If $B_1, \cdots, B_l$ are invariant sets each containing $X(\mathfrak{U})$ and if $A'(a)$ is an invariant neighborhood of $a$ contained in $A$, and $Y_{k+2}(\mathfrak{U})$ a chain such that*

$$Y(\mathfrak{U}) \subset B_i \qquad (i = 1, \cdots, l), \tag{1}$$

$$\phi\rho Y(\mathfrak{U}) = \rho X(\mathfrak{U}) \bmod M - A' + L,^4 \tag{2}$$

*then there exists a chain $\eta_{k+1}(\mathfrak{U})$ such that $\eta(\mathfrak{U}) \subset B_i$ $(i = 1, \cdots, l)$, $\eta(\mathfrak{U}) \subset L$, and $\phi\eta(\mathfrak{U}) = \gamma(\mathfrak{U}) \bmod M - A'$.*

PROOF. $\phi\rho X(\mathfrak{U}) = \rho\gamma(\mathfrak{U}) \bmod M - A$, and since $\gamma(\mathfrak{U}) \subset L$ so that $\rho\gamma(\mathfrak{U}) = 0$ (3.33), it follows that $\rho X(\mathfrak{U})$ is a cycle mod $M - A$ of type $(\rho, M - A)$. Let

$$Z(\mathfrak{U}) = X(\mathfrak{U}) - \phi Y(\mathfrak{U}). \tag{3}$$

Then from (2) it follows that $\rho Z(\mathfrak{U}) = 0 \bmod M - A' + L$. Hence we may write $Z(\mathfrak{U}) = \bar{\rho}W(\mathfrak{U}) \bmod M - A' + L$ (3.11). It is easy to see then that there exists a relation of the form

$$Z(\mathfrak{U}) = \bar{\rho}W(\mathfrak{U}) + \eta(\mathfrak{U}) + Z'(\mathfrak{U}) \tag{4}$$

where $\eta(\mathfrak{U}) \subset L$, $Z'(\mathfrak{U}) \subset M - A'$, $L \cap Z'(\mathfrak{U}) = 0$. On substituting (4) into (3) and operating by $\phi$ on both sides, we obtain

$$\phi\bar{\rho}W(\mathfrak{U}) = \gamma(\mathfrak{U}) - \phi\eta(\mathfrak{U}) \bmod M - A'.$$

The chain on the right is in $L$ whereas that on the left contains no simplex which is in $L$. Hence

$$\gamma(\mathfrak{U}) - \phi\eta(\mathfrak{U}) = 0 \qquad \bmod M - A'.$$

It remains to prove that $\eta(\mathfrak{U}) \subset B_i$ $(i = 1, \cdots, l)$. Since the right member of (3) is in $B_i$, so is $Z(\mathfrak{U})$. Now $(\rho W(\mathfrak{U}) + Z'(\mathfrak{U})) \cap L = 0$ so that $\rho W(\mathfrak{U}) + Z'(\mathfrak{U})$ has no simplex in common with $\eta(\mathfrak{U})$. Hence it follows from (4) that $\eta(\mathfrak{U}) \subset B_i$.[5]

---

[4] We do not write $\rho X(\mathfrak{U}) \simeq 0 \bmod M - A' + L$ in $B_i$ here, because according to our definitions this would impy that $M - A' + L \subset B_i$. Note that (1) does not necessarily imply that $Y(\mathfrak{U}) \subset B_1 B_2 \cdots B_l$.

[5] In the proof of lemma 2, use was made of the fact that when the coefficient field $\mathfrak{f}$ is $\mathfrak{p}$, no chain of the form $\sigma X$ or of the form $\bar{\sigma}X$ can contain a simplex in $L$ (3.33). This holds for chains of the latter type when $\mathfrak{f}$ is other than $\mathfrak{p}$ but does not in general hold for chains of the former type and therefore the lemma is not true for general $\mathfrak{f}$. It is this fact which up to the present has prevented us, except in special cases, from eliminating all restrictions on the period.

**6.2.** Our principal theorem concerning the local properties of $L$ can now be stated as follows:

THEOREM 1. *If the space $M$ is connected and of type $P_mQ$, then $L$ is of type $PQ$.*

The proof will occupy sections 6.3 to 6.14 and will consist of a sequence of steps quite similar to those which led to the results in the last part of our earlier paper. We shall only give details of proof when they are not fairly obvious modifications of the corresponding details in the earlier work. The key to the proof is the relationship, indicated in lemma 2, which exists between the *special* homologies in $M$ and the *ordinary* homologies in $L$.

**6.3.** We assume then that $M$ is connected and of type $P_mQ$. Let $d$ be an arbitrary but definitely chosen point of $L$. We must show that for suitable $r$, $M$ possesses properties $P_r$ and $Q$ at $d$. We may, and shall, assume that $d$ is not an inner point of $L$; for if the opposite were true $L$ would obviously possess properties $P_m$ and $Q$ at $d$.

Let $(D(d), {}^d\Omega_m)$ be a fundamental pair for $d$. Since $D$ may be replaced by a smaller neighborhood of $d$, we may assume that $D$ is invariant. Let $n = \dim M$. As we have remarked (5.2), $n \geqq m$. Let $\rho_0, \rho_1, \cdots, \rho_m$ stand alternately for $\sigma$ and $\bar{\sigma}$ if $m$ is even and for $\bar{\sigma}$ and $\sigma$ if $m$ is odd; in either case $\rho_m = \sigma$.

**6.4.** *Let $a$ be a point in $LD$ and $A(a)$ an invariant neighborhood of $a$ such that $A \subset D$. There exists an invariant $A'(a) \subset A$ with the property that* (1) *if $\Gamma_h(m+1 \leqq h \leqq n)$ is a cycle* mod $M - A$ *such that each $\Gamma_h(\mathfrak{U})$ is of type $(\rho, M - A)$, then $\Gamma_h \simeq 0$* mod $M - A' + L$; (2) *if $\Gamma_m$ is a cycle* mod $M - A$ *such that each $\Gamma_m(\mathfrak{U})$ is of type $(\rho, M - A)$ and such that $\Gamma_m \sim 0$* mod $M - A$, *then $\Gamma_m \simeq 0$* mod $M - A' + L$.

PROOF. Choose invariant neighborhoods $A_0, A_1, \cdots, A_n$ of $a$ such that $A = A_0 \supset A_1 \supset \cdots \supset A_n$ and such that every cycle mod $M - A_i$ of dimension $\neq m$ is $\sim 0$ mod $M - A_{i+1} (i = 0, \cdots, n-1)$. The $A$'s exist by virtue of property $P_m$ at $d$. Let $\Gamma_h (m \leqq h \leqq n)$ be a cycle such that every $\Gamma_h(\mathfrak{U})$ is of type $(\rho, M - A)$; in particular if $h = m$, assume that $\Gamma_h \sim 0$ mod $M - A$. In any case, $\Gamma_h \sim 0$ mod $M - A_1$, say $\Gamma_h = \phi X_{h+1}$ mod $M - A_1$. Since $\phi\bar{\rho}X_{h+1}(\mathfrak{U}) = \bar{\rho}\Gamma_h(\mathfrak{U}) = 0$ mod $M - A_1$ (3.11) it follows that $\rho_{h+1}X_{h+1}(\mathfrak{U})$ is a cycle mod $M - A_1$ of type $(\bar{\rho}, M - A_1)$. Consider a definite $\mathfrak{U}$. We may assume that the cycle $\bar{\rho}X_{h+1}(\mathfrak{U})$ is essential; for if it is not, all $\mathfrak{U}$-chains and $\mathfrak{U}$-cycles which have appeared in the argument can be replaced by invariant projections into $\mathfrak{U}$ of their coefficients in a special normal refinement of $\mathfrak{U}$, without affecting the boundary relations among them.[6] It follows that there exists an $(h+1)$-cycle mod $M - A_1$ of which $\bar{\rho}X_{h+1}(\mathfrak{U})$ is a coefficient and therefore $\bar{\rho}X_{h+1}(\mathfrak{U}) \sim 0$ mod $M - A_2$, say $\bar{\rho}X_{h+1}(\mathfrak{U}) = \phi X_{h+2}(\mathfrak{U})$ mod $M - A_2$.

[6] This process replaces $\Gamma(\mathfrak{U})$ by a cycle $\Gamma'(\mathfrak{U})$ which is $\sim\Gamma(\mathfrak{U})$ mod $M - A$ and therefore, strictly speaking, we no longer have the cycle $\Gamma$ we started with, but one homologous to it mod $M - A$. But since our investigation really concerns homology classes, it is quite proper to regard cycles in a given homology class as identical.

In the same way we may assume that $\rho X_{h+2}(\mathfrak{U})$, which is readily seen to be a cycle mod $M - A_1$, is essential and therefore $\sim 0 \bmod M - A_2$. This enables us to continue the building-up process. We finally obtain $\rho' X_n(\mathfrak{U})$ ($\rho' = \sigma$ or $\bar{\sigma}$), a cycle mod $M - A_{n-h-1}$ which is $\sim 0 \bmod M - A_{n-h}$. We have then $\rho' X_n(\mathfrak{U}) = 0 \simeq 0 \bmod M - A_{n-h} + L$ (see 6.0) and since

$$\rho' X_n(\mathfrak{U}) : \cdots : \rho_{h+2} X_{h+2}(\mathfrak{U}) : \bar{\rho}_{h+1} X_{h+1}(\mathfrak{U}) : \Gamma_h(\mathfrak{U})$$

(see 3.14), we have $\Gamma_h(\mathfrak{U}) \simeq 0 \bmod M - A_{n-h} + L$ (3.15). The same relation holds mod $M - A_n + L$ and therefore we may take $A' = A_n$.

**6.5.** *Let $A(d)$ be an invariant neighborhood of $d$. There exists an invariant $A'(d) \subset A$ with the property that for every invariant neighborhood $B(b)$ contained in $A'$, with $b \subset LA$, there exists an invariant $B'(b) \subset B$ such that every cycle* mod $M - A$ *in* $M - B$ *and of dimension* $\leqq n$ *and type* $(\rho, M - A)$ *is* $\simeq 0$ mod $M - A' + L$, *in* $M - B' + L$.

The proof is essentially the same as that of 6.4 except that now the building up process is based on property $Q$ rather than $P_m$.

**6.6.** Suppose there exists an invariant neighborhood $E(d)$ and a cycle ${}^d\Delta_m$ mod $M - E$ of type $(\rho_m, M - E + L)$ such that (1) $(E(d), {}^d\Delta_m)$ is a fundamental pair for $d$; (2) if $E'$ is an invariant non-null open subset of $E$, then $\Delta$ cannot be $\simeq 0$ mod $M - E' + L$; (3) for each invariant neighborhood $A(d)$ contained in $E$, there exists an invariant $A'(a) \subset A$ such that $\Delta$ constitutes a basis for $m$-cycles mod $M - A + L$ of type $(\rho_m, M - A + L)$ relative to special homologies mod $M - A' + L$. We shall call $(E(d), {}^d\Delta_m)$ a *special fundamental pair* for $d$.

*There exists a special fundamental pair for $d$.*

Proof. Since $D$ is invariant, $T({}^d\Omega_m)$ is also a cycle mod $M - D$. By property $P_m$, there exists a $D_0(d)$ which we may take to be invariant, such that $D_0 \subset D$ and $T\Omega_m \sim x\Omega_m \bmod M - D_0$ ($x \subset \mathfrak{p}$). Obviously $T^2\Omega \sim x\, T\Omega \bmod M - D_0$ so that $T^2\Omega \sim x^2\Omega \bmod M - D_0$ and finally $\Omega = T^p\Omega \sim x^p\Omega \bmod M - D_0$, which can only be true if $x = 1$. Thus $\bar{\rho}_m\Omega = \bar{\sigma}\Omega = \Omega - T\Omega \sim 0 \bmod M - D_0$. By 6.4 there exists an invariant $D_{00}(d) \subset D_0$ such that $\bar{\rho}_m\Omega \simeq 0 \bmod M - D_{00} + L$. Since no chain of the form $\bar{\rho}X$ can contain a simplex which is in $L$, it is easy to see that the last relation holds also mod $M - D_{00}$, say

$$\bar{\rho}_m\Omega(\mathfrak{U}) = \phi\bar{\rho}_m Y_{m+1}(\mathfrak{U}) \bmod M - D_{00}.$$

Let

$$\Delta_m(\mathfrak{U}) = \Omega_m(\mathfrak{U}) - \phi Y_{m+1}(\mathfrak{U}). \tag{1}$$

Obviously $\{\Delta_m(\mathfrak{U})\} = \Delta_m$ is a cycle mod $M - D$, homologous mod $M - D$ to ${}^d\Omega_m$. Moreover $\bar{\rho}_m\Delta_m = 0 \bmod M - D_{00}$ so that each $\Delta_m(\mathfrak{U})$ is of type $(\rho_m, M - D_{00} + L)$. By 6.4 there exists an invariant $E(d) \subset D_{00}$ such that every $m$-cycle mod $M - D_{00}$ whose coefficients are of type $(\rho_m, M - D_{00})$ and are $\sim 0 \bmod M - D_{00}$ is itself $\simeq 0 \bmod M - E + L$. Since $\Delta_m$ is a cycle

mod $M - D_{00}$, it follows that if $\pi$ is an invariant projection of $\mathfrak{V}$ into $\mathfrak{U}$ ($\mathfrak{V} \subset \mathfrak{U}$), $\pi\Delta_m(\mathfrak{V}) - \Delta_m(\mathfrak{U}) \sim 0 \bmod M - D_{00}$. Hence $\pi\Delta_m(\mathfrak{V}) - \Delta_m(\mathfrak{U}) \simeq 0 \bmod M - E + L$, therefore $\Delta_m$ satisfies the conditions for being a cycle mod $M - E + L$ of type $(\rho_m, M - E + L)$. Evidently $(E, \Delta)$ is a fundamental pair for $d$.

Suppose that $\Delta_m \simeq 0 \bmod M - E' + L$ where $0 \neq E' = TE' \subset E$. From lemma 1 there exists a cycle $\Delta'_m \bmod M - E'$ of type $(\rho_m, M - E')$ such that $\Delta'_m \simeq 0 \bmod M - E'$ and $\Delta_m = \Delta'_m \bmod L$. Since $d$ is not an inner point of $L$ and $L$ is closed, there can be chosen in $E'(d)$ a non-null open set $B$ such that $BL = 0$. Then $L \subset M - B$ so that $\Delta = \Delta' \bmod M - B$. Since $B \subset E'$ we have $\Delta' \simeq 0 \bmod M - B$, and since $\Delta \sim \Omega \bmod M - B$, we have $\Omega \sim 0 \bmod M - B$ which is impossible.—That $\Delta_m$ constitutes a basis of the stated type for special homologies follows readily from 6.4 and the fact that $(E, \Delta)$ is a fundamental pair for $d$.

**6.7.** Before we can complete the proof of theorem 1 we shall need the following theorem, which is of some interest in itself (cf. 3.36).

THEOREM 2. *Let $M$ be a connected space and $T$ a periodic homeomorphism of $M$ with itself of period $q$ where $q$ is either prime or composite. If $M$ is of type $P_mQ$ relative to the field $\mathfrak{p}$ where $p$ is a prime factor of $q$, then the set $L$ of fixed points is nowhere dense.*

PROOF. Assume first that $q = p =$ a prime. We shall show that the set $L_0$ of inner points of $L$ is null. Suppose $L_0 \neq 0$. Then since $M$ is connected, $L_0$ cannot be closed otherwise $L_0$ would equal $M$ and $T$ would be the identity transformation. It follows that $\bar{L}_0 - L_0 \neq 0$. Let $d_0$ be a point of $\bar{L}_0 - L_0$. Obviously $d_0$ is not an inner point of $L$. Now since the point $d$ introduced in 6.3 was assumed not to be an inner point of $L$ but otherwise was a perfectly arbitrary point of $L$, we may assume for the moment that $d = d_0$. Every neighborhood of $d$ then contains inner points of $L$. Let $(E(d), {}^d\Delta_m)$ be a special fundamental pair for $d$ and let $a$ be a point of $E$ which is an inner point of $L$, and let $A$ be an invariant neighborhood of $a$ such that $A \subset LE$, $d \subset M - A$. By Lemma 1 there exists a cycle $\Delta'_m \bmod M - E$ of type $(\rho_m, M - E)$ such that $\Delta' = {}^d\Delta_m \bmod L$. We may write $\Delta'(\mathfrak{U}) = \rho_m X_m(\mathfrak{U}) + Z(\mathfrak{U})$ where $Z(\mathfrak{U}) \subset M - E$. Since no simplex of $\rho_m X_m(\mathfrak{U})$ is in $L$, each simplex of $\Delta'(\mathfrak{U})$ which is in $A$—hence in $L$—is also in $M - E$. But since $A \subset E$, no simplex of $\Delta'(\mathfrak{U})$ is in $A$ and therefore $\Delta'(\mathfrak{U}) \subset M - A$. We may assume that $\Delta'(\mathfrak{U})$ is essential (see proof of 6.4) and therefore from property $Q$ at $d$, there exists an invariant $E'(d) \subset E$ such that $\Delta'(\mathfrak{U}) \sim 0 \bmod M - E'$. Hence $\Delta' = \{\Delta'(\mathfrak{U})\}$ is a cycle mod $M - E'$, each coefficient of which is of type $(\rho_m, M - E')$ and which itself is $\sim 0 \bmod M - E'$. Hence by 6.4 there exists an invariant $E''(d)$ such that $\Delta' \simeq 0 \bmod M - E'' + L$. Since $\Delta = \Delta' \bmod M - E'' + L$ we have ${}^d\Delta_m \simeq 0 \bmod M - E'' + L$, which is impossible (6.6). This completes the proof for prime $q$.

Suppose that $q = ps$, $p$ a prime. Then $T^s$ is a homeomorphism of $M$ with

itself of prime period $p$. Evidently the set $L^{(s)}$ of points invariant under $T^s$ contains $L$ and since $L^{(s)}$ is nowhere dense in $M$, the same is true of $L$.

**6.8.** We now continue with the proof of theorem 1. Let $(E(d), \Delta_m)$ be a special fundamental pair for $d$. Since $\Delta_m$ is of type $(\rho_m, M - E + L)$, we may write $\Delta_m = \rho_m\chi_m \bmod M - E + L$. Let $\Delta_{m-1} = \phi\chi_m$. Then $\Delta_{m-1}$ is a cycle mod $M - E + L$ of type $(\rho_{m-1}, M - E + L)$ (see 3.21). Thus we may write $\Delta_{m-1} = \rho_{m-1}\chi_{m-1} \bmod M - E + L$. Let $\Delta_{m-2} = \phi\chi_{m-1}$ and continue in this manner down to the dimension 0. We obtain a sequence $\Delta_m, \cdots, \Delta_0$ of cycles mod $M - E + L$ such that

$$\Delta_h = \rho_h\chi_h \bmod M - E + L \qquad (h = m, \cdots, 0),$$

$$\phi\chi_h = \Delta_{h-1} \qquad (h = m, \cdots, 1),$$

$$\Delta_m : \Delta_{m-1} : \cdots : \Delta_0 .$$

**6.9.** *Let $a$ be a point in $LE$ and $A(a)$ an invariant neighborhood contained in $E$. There exists an invariant $A'(a) \subset A$ such that each $\Delta_h$ constitutes a basis for cycles mod $M - A$ of type $(\rho_h, M - A)$ relative to special homologies* mod $M - A' + L$.

PROOF. It will be sufficient to show that for each $k$ $(0 \leqq k \leqq m)$ there exists an invariant $A_k(a) \subset A$ such that every $\Delta_h$ with $k \leqq h \leqq m$ constitutes a basis for cycles mod $M - A$ of type $(\rho_h, M - A)$ relative to special homologies mod $M - A_h + L$. Stated in this form the theorem follows for $k = m$ from the properties of $(E, \Delta_m)$ (6.6) and the obvious fact that cycles of type $(\rho_h, M - A)$ are also of type $(\rho_h, M - A + L)$. For smaller values of $k$, the theorem is proved by induction (cf. proof of 3.40) based on 3.15 and the following modification of 3.24:

*Let $a$ be a point of $LE$ and $A$ an invariant neighborhood of $a$ such that $A \subset E$. There exists an invariant $A'(a) \subset A$ such that if $\Gamma_h$ is a cycle* mod $M - A$ *of type $(\rho_h, M - A)$ with $h < m$, there exists a cycle* mod $M - A'$ *of type $(\rho_{h+1}, M - A')$ such that $\Gamma_{h+1} : \Gamma'_h$ and $\Gamma_h \simeq \Gamma'_h$* mod $M - A'$.

When $h < m - 1$, the proof of this lemma is essentially the same as that of 3.24 except that we now make use of property $P_m$ instead of III, 3.24, to show that certain (relative) cycles of dimensions $h$ and $h + 1$ are $\sim 0$. For the dimension $m - 1$ the proof is essentially the same as that of 3.39 for the dimension $n - 1$.[7]

**6.10.** *There exists an invariant neighborhood $F(d) \subset E(d)$ and an integer $r$ $(0 \leqq r \leqq m - 1)$ such that* (1) $\Delta_r \simeq 0$ mod $M - F + L$ *and* (2) *if $A(a)$ is an invariant neighborhood such that $a \subset FL$, $A \subset F$, then $\Delta_h$ cannot be $\simeq 0$* mod $M - A + L$ *if $h > r$.*

[7] The argument in 3.39 is not quite accurate but may be made so as follows: we observe first that under the hypothesis that $\Gamma_{n-1}$ is not $\simeq 0$, the totality of coverings $\mathfrak{U}$ for which $\Gamma_{n-1}(\mathfrak{U})$ is not $\simeq 0$ is a complete system and we may assume that all coverings which appear in the argument belong to that system.

PROOF. Let $F(d)$ be an invariant neighborhood of $d$ such that $F \subset E$ and such that if $B(b)$ is an invariant neighborhood contained in $F$, with $b \subset LF$, then every cycle mod $M - F$ of type $(\rho, M - F)$ and dimension $\leqq n$ is $\simeq 0$ mod $M - F + L$. Such an $F$ exists by 6.5. In the sequence $\Delta_m, \Delta_{m-1}, \cdots, \Delta_0$ let $\Delta_r$ be the first cycle which is $\simeq 0$ mod $M - F + L$; the sequence actually contains such a cycle since $\Delta_0 \simeq 0$ mod $M - F + L$ (see 3.48). We shall show that $F$ and $\Delta_r$ have the required properties.

It follows from the properties of special fundamental pairs that $r < m$. It remains to show that if $h > r$ there can exist no relation of the form

$$\Delta_r \simeq 0 \bmod M - A + L, \tag{1}$$

where $A = A(a) \subset F$, $a \subset LF$, $A = TA$. From lemma 1 we may write $\Delta_h(\mathfrak{U}) = \Delta'_h(\mathfrak{U})$ mod $L$ where $\Delta'(\mathfrak{U})$ is a cycle mod $M - E$ of type $(\rho_h, M - E)$. Suppose now that (1) does hold for some $A$. Then from lemma 1,

$$\Delta'(\mathfrak{U}) \simeq 0 \bmod M - A$$

for every $U$. Hence there exist chains $X_{h+1}(\mathfrak{U})$ such that $\Delta'(\mathfrak{U}) = \phi\rho_h X_{h+1}(\mathfrak{U})$ mod $M - A$. Let $P(\mathfrak{U}) = A \cap \Delta'_h(\mathfrak{U})$, $Q(\mathfrak{U}) = \Delta_h(\mathfrak{U}) - P(\mathfrak{U})$. Then $\phi\rho_h X_{h+1}(\mathfrak{U}) = P(\mathfrak{U})$ mod $M - A$ since $Q(\mathfrak{U}) = 0$ mod $M - A$. Thus

$$\phi\rho_h X_{h+1}(\mathfrak{U}) = P(\mathfrak{U}) + H(\mathfrak{U}) \tag{2}$$

say, where $H(\mathfrak{U}) \subset M - A$. Since $\phi P(\mathfrak{U}) = -\phi H(\mathfrak{U})$ and $\phi P(\mathfrak{U}) = -\phi Q(\mathfrak{U})$, the chain $Q(\mathfrak{U}) - H(\mathfrak{U})$ is an absolute cycle in $M - A$. Now since $\Delta'_h(\mathfrak{U})$ is of type $(\rho_h, M - E)$ it is easy to see that $P(\mathfrak{U})$ and $Q(\mathfrak{U})$ must likewise be of type $(\rho_h, M - E)$ and hence the same is true of $H(\mathfrak{U}) = \phi\rho_h X_{h+1}(\mathfrak{U}) - P(\mathfrak{U})$, and hence of $Q(\mathfrak{U}) - H(\mathfrak{U})$. We may assume (see proof of 6.4) that $Q(\mathfrak{U}) - H(\mathfrak{U})$, a cycle mod $M - E$ of type $(\rho_h, M - E)$ in $M - A$, is essential relative to special homologies and is therefore a coefficient of a cycle $\Gamma_h$ mod $M - E$, type $(\rho_h, M - E)$ in $M - A$. By the choice of $F$, we have $\Gamma_h \simeq 0$ mod $M - F + L$, hence $Q(\mathfrak{U}) - H(\mathfrak{U}) \simeq 0$ mod $M - F + L$. On adding this relation to the relation $P(\mathfrak{U}) + H(\mathfrak{U}) \simeq 0$ mod $M - F + L$ which follows from (2), we have $\Delta'_h(\mathfrak{U}) \simeq 0$ mod $M - F + L$. Hence $\Delta_h(\mathfrak{U}) \simeq 0$ mod $M - F + L$ for each $\mathfrak{U}$, which is impossible since $h > r$.

**6.11.** *There exists an invariant neighborhood $G(d) \subset F$ and an $r$-cycle $\delta_r$ mod $L(M - G)$ in $L$, which is not $\sim 0$ mod $L(M - G')$ in $L$ for any invariant open subset $G'$ of $G$ with $LG' \neq 0$.*

PROOF. Assume first that $m \leqq m - 2$. Since $\Delta_r \simeq 0$ mod $M - F + L$, we may write $\Delta_r = \phi\rho_r H_{r+1}$ mod $M - F + L$. Since $\Delta_r = \phi\chi_{r+1}$ (6.8), the chain $X'_{r+1}(\mathfrak{U}) = \rho_r H_{r+1}(\mathfrak{U}) - \chi_{r+1}(\mathfrak{U})$ is a cycle mod $M - F + L$. Let $\mathfrak{U}_1$ be a normal refinement of $\mathfrak{U}$ relative to cycles mod $M - F + L$ and let $X_{r+1}(\mathfrak{U}) = \pi X'_{r+1}(\mathfrak{U}_1)$ where $\pi = \pi(\mathfrak{U}_1, \mathfrak{U})$. By property $P_m$ at $d$, there exists an invariant $G(d) \subset F$ such that all $(r + 1)$-cycles mod $M - F$ are $\sim 0$ mod $M - G$. It

follows from an obvious modification of 1.6 that $X_{r+1} = \{X_{r+1}(\mathfrak{U})\}$ is a cycle mod $M - G + L$. We have

$$\begin{aligned}\rho_{r+1}X_{r+1}(\mathfrak{U}) &= \pi\bar{\rho}_r\rho_r H_{r+1}(\mathfrak{U}_1) - \pi\rho_{r+1}\chi_{r+1}(\mathfrak{U}_1) \\ &= \pi\Delta_{r+1}(\mathfrak{U}_1) \simeq \Delta_{r+1}(\mathfrak{U}) \bmod M - F + L.\end{aligned} \tag{1}$$

Suppose $X_{r+1} \sim 0 \bmod M - G' + L$; then by 3.16 $\rho_{r+1}X_{r+1} \simeq 0 \bmod M - G' + L$. Hence by (1), $\Delta_{r+1} \simeq 0 \bmod M - G' + L$ which is impossible. We conclude that $X_{r+1}$ cannot be $\sim 0 \bmod M - G' + L$.

By 1.1 (with $K = M - G$) there exists a cycle $\delta_r \bmod L(M - G)$ in $L$ and a cycle $X'_{r+1} \bmod M - G + L$ such that $\phi X'_{r+1} = \delta_r \bmod M - G$ and $X' \sim X \bmod M - G + L$. Suppose $\delta_r \sim 0 \bmod L(M - G')$ in $L$ where $G' \subset G$, $G'L \neq 0$. On account of property $P_m$ and the fact that $r + 1 < m$, there exists an open $G'' \subset G'$ with $G''L \neq 0$ such that every $(r + 1)$-cycle mod $M - G'$ is $\sim 0 \bmod M - G''$. Hence from an obvious modification of theorem 1.3[8] we conclude that $X_{r+1} \sim 0 \bmod M - G'' + L$ which is impossible.

For $r = m - 1$, the proof is quite similar to that of 4.3 and may be omitted.

**6.12.** *Let $A$ be a neighborhood of $a$ such that $a \subset GL$, $A \subset G$. There exists an $A'(a) \subset A$ such that $\delta_r$ constitutes a basis for $r$-cycles* mod $L(M - A)$ *in $L$ relative to homologies* mod $L(M - A')$ *in $L$.*

PROOF. For $r \leqq m - 2$ the proof is quite similar to that of 4.7 for $r \leqq n - 2$. For $r = m - 1$ we must give a separate proof because in 4.7 the proof of the corresponding case depends on assumption VI, 4.4, which plays no part in the present development.

Suppose then that $r = m - 1$. Let $\gamma_{m-1}$ be a cycle mod $L(M - A)$ in $L$. By property $P_m$ there exists an $A_1(a) \subset A$ such that $\gamma_{m-1} \sim 0 \bmod M - A_1$ and $\delta_{m-1} \sim 0 \bmod M - A_1$, say $\delta(\mathfrak{U}) = \phi X_m(\mathfrak{U}) \bmod M - A_1$ and $\gamma(\mathfrak{U}) = \phi Y_m(\mathfrak{U}) \bmod M - A_1$ for each $\mathfrak{U}$. Obviously we may take $A_1$ to be invariant. Then $\rho_m X(\mathfrak{U})$ and $\rho_m Y(\mathfrak{U})$ are cycles mod $M - A_1$ of type $(\rho_m, M - A_1)$; for $\phi\rho_m X(\mathfrak{U}) = \rho_m\gamma \bmod M - A_1$ and $\rho_m\gamma = \sigma\gamma = p\gamma = 0 \pmod p$. Since these cycles may be assumed to be essential (cf. proof of 6.4) there exists an invariant $A'(a) \subset A_1$ such that

$$\rho_m X_m(\mathfrak{U}) \simeq u_x\Delta_m(\mathfrak{U}) \bmod M - A' + L \tag{1}$$

$$\rho_m Y_m(\mathfrak{U}) \simeq u_y\Delta_m(\mathfrak{U}) \bmod M - A' + L, \tag{2}$$

$u_x$ and $u_y$ depending on $\mathfrak{U}$.

If $\zeta(\mathfrak{U}) \subset L$, let us write "$\zeta(\mathfrak{U}) \sim_* 0 \bmod L(M - A')$ in $L$" if there exists a chain $\eta(\mathfrak{U})$ such that $\eta(\mathfrak{U}) \subset L$, $\eta(\mathfrak{U}) \subset M - A'$, $\phi\eta(\mathfrak{U}) = \zeta(\mathfrak{U}) \bmod M - A'$. Since $\delta_r$ is not $\sim 0 \bmod L(M - A')$ in $L$, it follows from theorem B (5.1) that

[8] MODIFIED THEOREM. *Let $K$ and $L$ be sets in $M$ and $\gamma_h$ a cycle* mod $KL$ *in $L$. Let $X_{h+1}$ be a cycle* mod $K + L$ *such that $\phi X = \gamma$ mod $K$. If $\gamma \sim 0$ mod $KL$ in $L$ and if there exists a set $K' \supset K$ such that every $(h + 1)$-cycle* mod $K$ *is $\sim 0$ mod $K'$, then $X \sim 0$ mod $K' + L$.*— In the application above take $K = M - G'$, $K' = M - G''$, $h = r$.

for each $\mathfrak{U}$ there exists a refinement $\mathfrak{V}$ such that $\delta_r(\mathfrak{V})$ is not $\sim^* 0$ mod $L(M - A')$ in $L$. Let $v_x$, $v_y$ denote the coefficients entering (1) and (2) when $\mathfrak{U}$ is replaced by $\mathfrak{V}$. Suppose $v_x = 0$. Then by lemma 2 there exists a chain $\eta_m(\mathfrak{V})$ such that $\phi\eta(\mathfrak{V}) = \delta(\mathfrak{V})$ mod $M - A'$ and $\eta(\mathfrak{V}) \subset L$. Since $\{\mathfrak{V}\}$ is a complete system, it follows from 5.1, theorem B, that $\delta \sim 0$ mod $L(M - A')$ in $L$, which is impossible. We conclude that $v_x \neq 0$. From (1) and (2) we have

$$v_y\rho_m X_m(\mathfrak{V}) - v_x\rho_m Y_m(\mathfrak{V}) \simeq 0 \bmod M - A' + L.$$

Hence by another application of lemma 2 we obtain the relation

$$v_y\delta(\mathfrak{V}) - v_x\gamma(\mathfrak{V}) \sim^* 0 \bmod L(M - A') \text{ in } L.$$

Since $v_x \neq 0$, we may write

$$\gamma(\mathfrak{V}) \sim^* v\,\delta(\mathfrak{V}) \bmod L(M - A') \text{ in } L. \tag{3}$$

Suppose $\mathfrak{V}_1$, $\mathfrak{V}_2$ are $\mathfrak{V}$'s such that $\mathfrak{V}_2 \subset \mathfrak{V}_1$. Let $v_1$, $v_2$ be the corresponding coefficients in (3) and let $\pi = \pi(\mathfrak{V}_2, \mathfrak{V}_1)$. Then

$$\gamma(\mathfrak{V}_1) \sim^* \gamma(\mathfrak{V}_2) \sim^* \pi\delta(\mathfrak{V}_2) \sim^* \delta(\mathfrak{V}_1) \bmod L(M - A') \text{ in } L.$$

Hence

$$(v_2 - v_1)\delta(\mathfrak{V}_1) \sim^* 0 \bmod (M - A')L \text{ in } L$$

which can only be true if $v_1 = v_2$. Suppose now that $\mathfrak{V}_2$ is an *arbitrary* $\mathfrak{V}$. Then we still have $v_1 = v_2$ because both numbers are equal to $v_3$ say corresponding to $\mathfrak{V}_3 \subset \mathfrak{V}_1\mathfrak{V}_2$. Thus the coefficient $v$ in (3) is independent of $\mathfrak{V}$ and it follows that $\gamma \sim^* v\delta$ mod $L(M - A')$ in $L$. Since $\{\mathfrak{V}\}$ is a complete system, we conclude from theorem B (5.1) that $\gamma \sim v\delta$ mod $L(M - A')$ in $L$.

**6.13.** *Let $a$ be a point in $LG$ and $A$ a neighborhood of $a$ such that $A \subset G$. There exists an $A'(a)$ such that every cycle* mod $L(M - A)$ *in $L$ and of dimension $\neq r$, is $\sim 0$* mod $L(M - A')$ *in $L$.*

Proof. Let $\gamma_h$ be a cycle mod $L(M - A)$ in $L$, with $h \neq r$. There exists an invariant $A_1(a)$ and chains $X_{h+1}(\mathfrak{U})$ such that $\phi X_{h+1}(\mathfrak{U}) = \gamma_h(\mathfrak{U})$ mod $M - A_1$. When $h \neq m$, this follows from the fact that $(G(d), \Delta_m)$ is a fundamental pair; for $h = m$ we prove it as follows. Since (by theorem 2) $L$ is nowhere dense, there exists a neighborhood $B(b)$ such that $B \subset A$, $BL = 0$. Then $\gamma_m \subset M - B$ and our assertion follows from property $Q$.—Now $\rho_{h+1}X_{h+1}(\mathfrak{U})$, a cycle mod $M - A_1 + L$ of type $(\rho_{h+1}, M - A_1 + L)$, may be assumed to be essential relative to special homologies mod $M - A_1 + L$. Hence $\rho_{h+1}X_{h+1}(\mathfrak{U})$ is a coefficient of a cycle of type $(\rho_{h+1}, M - A_1 + L)$ and therefore (6.9) there exists an invariant $A'(a) \subset A_1$ such that

$$\rho_{h+1}X_{h+1}(\mathfrak{U}) \simeq u\Delta_{h+1}(\mathfrak{U}) \bmod M - A' + L \tag{1}$$

where $u$ depends on $\mathfrak{U}$ but $A'$ is independent of $\mathfrak{U}$ and of $X_{h+1}$. If $h \leqq r - 1$, the right side of (1) is $\simeq 0$ by definition of $r$ and hence

$$\rho_{h+1}X_{h+1}(\mathfrak{U}) \simeq 0 \bmod M - A' + L. \tag{2}$$

We shall show that (2) holds also when $h > r$. For such an $h$, $\Delta_h$ is not $\simeq 0$ mod $M - A' + L$ and hence for each $\mathfrak{U}$ there exists a special refinement $\mathfrak{V}$ such that $\Delta_h(\mathfrak{V})$ is not $\simeq 0$ mod $M - A' + L$. On writing $\mathfrak{V}$, $v$ in place of $\mathfrak{U}$, $u$ in (1) and applying 3.15 we obtain

$$v\Delta_h(\mathfrak{V}) \simeq \gamma_h(\mathfrak{V}) \text{ mod } M - A' + L.$$

Since $\gamma(\mathfrak{V}) \subset L$, we have $v\Delta_h(\mathfrak{V}) \simeq 0$ mod $M - A' + L$, which can only be true if $v = 0$. Thus (2) still holds, at least if $\mathfrak{U}$ is replaced by $\mathfrak{V}$. From lemma 2 there exists an $\eta(\mathfrak{V})$ in $L$ such that $\phi\eta(\mathfrak{V}) = \gamma(\mathfrak{V})$ mod $M - A'$ and since $\{\mathfrak{V}\}$ is a complete system we have (5.1, theorem B) $\gamma \sim 0$ mod $L(M - A')$ in $L$.

**6.14.** It is a consequence of 6.11, 6.12, 6.13 that $L$ possesses the property $P_r$ at $d$; in fact $(LG(d), \delta_r)$ is a fundamental pair in $L$ for $d$. It remains to show that $L$ possesses the property $Q$ at $d$.

To prove this, let $A$ be an invariant neighborhood of $d$. By property $Q$ at $d$, there exists an invariant $A_1(d)$ such that for every invariant $C(a)$ with $a \subset LA_1$, $C \subset A$, there exists an invariant $C_1(a) \subset C$ with the property that all cycles mod $M - A$ in $M - C$ are $\sim 0$ mod $M - A_1$ in $M - C_1$. By 6.5 there exists an invariant $A'(d) \subset A_1$ such that for every invariant $C_1(c_1)$ with $c_1 \subset LA'$, $C_1 \subset A'$, there exists an invariant $C'(c_1)$ with the property that all cycles mod $M - A_1$ in $M - C_1$ and of type $(\rho, M - A_1)$ are $\simeq 0$ mod $M - A' + L$ in $M - C' + L$. Let $b$ be a point in $LA'$ and $B(b)$ an invariant neighborhood of $b$, such that $LB \subset LA'$. Our theorem will be established if we show that $\gamma \sim 0$ mod $L(M - A')$ in $L(M - B')$ where $B'$ is independent of $\gamma$.[9] On replacing $B$ by $A'B$ if necessary, we may suppose that $B \subset A'$. Since $\gamma$ is a cycle mod $M - A$ in $M - B$ and $B \subset A_1$, there exists an invariant $B_1(b) \subset B$ and chains $X(U)$ in $M - B_1$ such that $\phi X = \gamma$ mod $M - A_1$. Then $\rho X$ is a cycle mod $M - A_1$ of type $(\rho, M - A_1)$ (see 3.47) and may be assumed to be essential relative to special homologies. Therefore, since $B_1 \subset A'$, there exists an invariant $B'(b) \subset B_1$ such that $\rho X \simeq 0$ mod $M - A' + L$ in $M - B' + L$. From lemma 2 we may write $\gamma(\mathfrak{U}) = \phi\eta(\mathfrak{U})$, where $\eta(\mathfrak{U}) \subset M - B'$, $\eta(\mathfrak{U}) \subset L$. Since $\{\mathfrak{U}\}$ is a complete system, it follows from theorem B (5.1) that $\gamma \sim 0$ mod $L(M - A')$ in $L(M - B')$.

*The proof of the theorem* 1 *is now complete.*

**6.15.** *If $T$ is of prime period $p$ and $M$ is* HLC$^n$ *(relative to* $\mathfrak{p}$*) where $n = \dim M$, then $L$ is* HLC$^n$.

Proof. By means of a building-up process followed by a splitting down process we can show readily that if $M$ is HLC$^n$, there exists for every invariant $A(a)$, $a \subset L$, an invariant $A'(a) \subset A$ such that every cycle of type $\rho$ in $A'$ and of dimension $\leqq n$, is $\simeq 0$ mod $L$ in $A$. The theorem then follows from an application of lemma 2. (See for example the proof of 6.4.)

[9] The fact that $A$ is invariant does not prevent $LA$ from being a perfectly arbitrary neighborhood in $L$ of $d$. For suppose $B$ is an open set such that $d \subset LB$. Let $A = B + TB + \cdots + T^{p-1}B$. Then $A$ is invariant and $d \subset LA = LB$.

THEOREM 3. *Let $T$ be a periodic homeomorphism of a connected space $M$ with itself, $T$ being of period $p^\alpha$, $p$ a prime. Let $n = \dim M$ and let $L$ be the set of fixed points. If $M$ is* HLC$^n$ *relative to* $\mathfrak{p}$, *then $L$ has a finite number of components and each component is* HLC$^n$. *If in addition $M$ is of type $P_mQ$ (relative to* $\mathfrak{p}$), *each component of $L$ is of type $P_rQ$, $r$ depending on the component.*

PROOF. If $\alpha = 1$, the theorem follows from 5.4, 5.5, 5.6, 6.15.

Suppose that the theorem is true for all transformations of period $p^\beta$, $\beta \leqq \alpha - 1$. The transformation $T^q$ where $q = p^{\alpha-1}$ is of period $p$ and therefore if $M$ is HLC$^n$, the set $\mu$ of fixed points of $T^q$ has a finite number of components and each component is HLC$^n$. If in addition $M$ is of type $P_mQ$, each component is of type $P_rQ$. Now $T$ transforms $\mu$ into itself. For if $x$ is invariant under $T^q$, we have $T^q(Tx) = T(T^qx) = Tx$ so that $Tx$ is also invariant under $T^q$. Thus $T$ permutes the components of $\mu$ among themselves; in particular, the components of $\mu$ which contain points of $L$ are transformed into themselves by $T$. Let these components be $\mu_1, \cdots, \mu_l$ and let $T_i$ be the transformation induced by $T$ in $\mu_i$. Let $L_i$ be the set of points in $\mu_i$ which are fixed under $T_i$. Since $L \subset \sum L_i$ and since each point which is invariant under $T_i$ is invariant under $T$, we have $L = \sum L_i$. Consider a definite value of $i$ and assume that $M$ is HLC$^n$ so that $\mu_i$ is HLC$^n$. Since $T_i^q$ is the identity (in $\mu_i$), $T_i$ is either the identity or is of period $p^\beta$ where $\beta \leqq \alpha - 1$. In the former case we have $\mu_i = L_i$ so that $L_i$ is HLC$^n$; in the latter, it follows from the hypothesis of the induction that $L_i$ is HLC$^n$. Thus each $L_i$—and hence $L$—is HLC$^n$ and $L$ therefore has a finite number of HLC$^n$ components. If we assume that $M$ is of type $P_mQ$ as well as HLC$^n$, then $\mu_i$ is of type $P_sQ$ ($s = s_i$) and therefore the components, $L_{ij}$ say, of $L_i$ are of type $P_rQ$, $r$ depending on the component. Since $L = \sum L_i = \sum L_{ij}$, the theorem is now proved.[10]

**6.16.** Suppose that $T$ is of period $p^\alpha$ and that $M$ is metric. Suppose further that $M$ is HLC$^n$ and of type $P_mQ$ relative to $\mathfrak{p}$. If the component $L_i$ of $L$ is of type $P_{r_i}Q$, then $\dim_{\mathfrak{p}} L_i = r_i$ (5.2). Since $\dim_{\mathfrak{p}} L_i \leqq \dim L_i$, components of dimension 0 are of type $P_0$ and hence are points (5.3). If $L_i$ is of dimension 1, then $r_i = \dim_{\mathfrak{p}} L_i \leqq 1$. Hence by 5.3, $r_i = 1$ and therefore the 0- and 1-dimensional local Betti number relative to $\mathfrak{p}$ at an arbitrary point $x$ of $L$ are 0 and 1 respectively and so are the Betti numbers around $x$ (Alexandroff [8]). From this it follows that if $M$ is assumed to be metric, every 1-dimensional component of $L$ is a simple closed curve (see 4.11, footnote 12). Hence

*If $T$ is of period $p^\alpha$ and if $M$ is metric and is* HLC$^n$ *and of type $P_mQ$ relative to* $\mathfrak{p}$, *the* 0- *and* 1-*dimensional components of $L$ are points and simple closed curves.*

**7.1.** *Periodic transformations of a* 3-*sphere.* It might perhaps be expected that in restricted cases at least the nature of the two-dimensional components

[10] This method of passing from the period $p$ to the period $p^\alpha$ is also applicable to the work in our earlier paper and therefore the results obtained there hold for transformations of period $p^\alpha$ and homologies relative to $\mathfrak{p}$.

could be determined as completely as that of the 0- and 1-dimensional components. We shall see that this is actually possible if $M$ is 3-dimensional and locally euclidean. In fact, with the aid of R. L. Wilder's theory of generalized closed manifolds (g.c.m.'s) it can be shown that for such an $M$ the two-dimensional components are closed surfaces. In order to keep details at a minimum we shall only consider the case in which $M$ is a euclidean 3-sphere; it will be seen that the method of treatment applies, at least in principle, to the case of arbitrary compact locally euclidean 3-spaces.[11]

**7.2.** Let $\sigma_\epsilon(a)$ denote the spherical neighborhood of radius $\epsilon$ about the point $a$ in a given metric space. The boundary points of $\sigma_\epsilon(a)$ are the points which are at a distance exactly $\epsilon$ from $a$; let their totality be denoted by $f_\epsilon(a)$.

Let us recall the definition of generalized closed manifold given by Wilder. An $n$-dimensional g.c.m. (relative to the coefficient field f) is a compact metric space $K$ such that

1. dim $K = n$;

2. $B_n(K) = 1$ *and* $B_n(K') = 0$ *for every closed proper subset* $K'$ *of* $K$. (*B denotes the Betti number over* f.)

3. *For every point* $a$ *of* $K$ *there is an* $\epsilon = \epsilon(a)$ *such that every h-cycle* $(1 \leqq h \leqq n-1)$ *in* $\sigma_\epsilon(a)$ *is* $\sim 0$ *in* $K$.

4. *For every point* $a$ *in* $K$ *and* $\epsilon > 0$, *there exist numbers* $\delta$, $\tau$ (*depending on* $a$) *such that* $\tau < \delta < \epsilon$ *and such that every h-cycle* $(0 \leqq h \leqq n-2)$ *in* $f_\delta(a)$ *is* $\sim 0$ *in* $\sigma_\epsilon(a) - \sigma_\tau(a)$ *and every* $(n-1)$*-cycle in* $f_\delta(a)$ *is* $\sim 0$ *in* $K - \sigma_\tau(a)$.

Wilder has shown (l.c. p. 903 after theorem 19) that *every 2-dimensional g.c.m. in in a euclidean 3-sphere is a closed surface.* In this theorem, the coefficient field may be either the rational numbers or $\mathfrak{p}$ (see Wilder's footnote 6).

**7.3.** Let $M$ be a euclidean 3-sphere and suppose that $T$ is of prime period $p$ and that dim $L = 2$. Then (4.15, 4.16) $L$ is connected and possesses the same (mod $p$) Betti numbers as a 2-sphere. *We now assert that* $L$ *is a 2-dimensional g.c.m.*

PROOF. We shall show that $L$ satisfies conditions (2) (3) (4) in the definition of a 2-dimensional g.c.m.

2. We have already remarked that $B_2(L) = 2 \pmod p$. It remains to show that if $L'$ is a closed proper subset of $L$, $B_2(L') = 0$.

$M_3$ has the obvious property that if $A$ is a non-null open set in $M_3$, every cycle in $M - A$ is $\sim 0$ (in $M$). By an argument very similar to that used in the proof of 6.14, we see that this property holds also in $L$. In particular every 2-cycle in $L(M - A)$ where $LA \neq 0$, is $\sim 0$ in $L$. Now since $L - L'$

[11] Wilder's theory (Annals of Math. 35 (1934), pp. 876–903) applies to sets $L$ immersed in a euclidean $n$-space or, what amounts essentially to the same thing, in a euclidean $n$-sphere. In order to arrive at conclusions concerning $L$ when the containing space $M$ is locally euclidean, not necessarily a sphere, a number of minor modifications in the theory are necessary.

is open (in $L$) and non-null, every cycle in $L'$ is $\sim 0$ in $L$. Let $\{\mathfrak{u}\}$ be the totality of finite coverings of $L$ by sets open in $L$ and let $\gamma = \{\gamma(\mathfrak{u})\}$ be a 2-cycle in $L'$. Each $\mathfrak{u}$ possesses a refinement $\mathfrak{u}_1$ of order $\leqq 3$ and since $\gamma \sim 0$, it follows that $\gamma(\mathfrak{u}_1) = 0$ for each $\mathfrak{u}_1$. Let $\pi = \pi(\mathfrak{u}_1, \mathfrak{u})$. Since $\gamma \subset L'$, we have $\gamma(\mathfrak{u}) \sim \pi\gamma(\mathfrak{u}_1)$ in $L'$, i.e. $\gamma(\mathfrak{u}) \sim 0$ in $L'$. Hence $\gamma \sim 0$ in $L'$ and 2 is verified.

3. This follows from the fact that $L$ is HLC$^3$ (6.15).

4. Let $S_\epsilon(a)$ denote a spherical neighborhood of radius $\epsilon$ in $M_3$ and let $F_\epsilon(a)$ be its boundary. To show that $L$ satisfies (4) it will be sufficient to verify 4′ and 4″ stated below.

4′. *Let $a$ be a point in $L$ and $\epsilon$ a number $> 0$. There exist $\delta$ and $\tau$, with $\epsilon > \delta > \tau$, such that every 0-cycle in $LF_\delta(a)$ is $\sim 0$ in $L(S_\epsilon(a) - S_\tau(a))$.*

Proof. Let $\sum_\epsilon(a)$ denote the invariant neighborhood $S + TS + \cdots + T^{p-1}S$ where $S = S_\epsilon(a)$. Obviously $L\sum_\epsilon(a) = LS_\epsilon(a)$. Let $\rho_3, \cdots, \rho_0$ be defined so that $\rho_3 = \sigma$.

We now choose numbers $\epsilon_0, \cdots, \epsilon_5$ such that (i) $\overline{\sum_1} \subset \sum_0$ (where $\sum_i$, $(F_i)$ mean $\sum_{\epsilon_i}$, $(F_{\epsilon_i})$); (ii) every cycle in $\sum_2$ of type $\rho$ is $\simeq 0 \bmod L$ in $\sum_1 + L$; (iii) $F_3 \subset \sum_2$; (iv) $\sum_4 \subset S_3 \cdot TS_3 \cdots T^{p-1}S_3$; (v) every 2-cycle mod $M - \sum_4$ of type $(\rho_1, M - \sum_4)$ is $\simeq 0 \bmod M - \sum_5 + L$. The possibility of fulfilling (ii) can be readily established by methods which are by now familiar (cf. 6.5 and the proof of 6.4). The possibility of fulfilling (v) is shown as follows. From the theorem in 3.46, there can be chosen a $\sum_5 \subset \sum_4$ such that every 2-cycle mod $M - \sum_4$ of type $(\rho_2, M - \sum_4)$ is $\simeq x\Delta_2 \bmod M - \sum_5 + L$ where $\Delta_2$ is defined in 3.32. But since $\dim_{\mathfrak{p}} L = \dim L$ (because $M$ is a euclidean 3-sphere) and since $\dim_{\mathfrak{p}} = r(\mathfrak{p})$ (4.11) we conclude that $r(\mathfrak{p}) = 2$ and hence (3.48) $\Delta_2 \simeq 0 \bmod M - \sum_5 + L$.—We shall show that for $\delta$, $\tau$ in condition 4′ we may take $\epsilon_0$, $\epsilon_5$. For this we must show that if $\gamma_0$ is a 0-cycle in $LF_3$, then $\gamma_0 \sim 0$ in $L(S_0 - S_5)$.

Since $\gamma_0 \subset F_3$ and $F_3$ is homeomorphic to an ordinary sphere, $\gamma_0 \sim 0$ in $F_3$. Thus we may write $\gamma_0 = \phi X_1$, $X_1 \subset F_3$. Hence $\rho_1 X_1(\mathfrak{U})$ is a cycle of type $\rho_1$ and by (iii) $\rho_1 X_1(\mathfrak{U}) \subset \sum_2$. We may assume that $\rho_1 X_1(\mathfrak{U})$ is essential relative to special homologies and hence by (ii) $\rho_1 X_1(\mathfrak{U}) \simeq 0 \bmod L$ in $\sum_1 + L$. Thus there exists a relation of the form $\phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U}) + \alpha(\mathfrak{U})$ where $\rho_1 X_2(\mathfrak{U}) \subset \sum_1 + L$, $\alpha(\mathfrak{U}) \subset L$. Since $L \cap \rho_1 X_2(\mathfrak{U}) = 0$, we have $\rho_1 X_2(\mathfrak{U}) \subset \sum_1$. Since also $L \cap \rho_1 X_1(\mathfrak{U}) = 0$, we have $\alpha(\mathfrak{U}) = 0$, and therefore $\phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U})$. In this relation, *we may assume that* $X_2(\mathfrak{U}) \subset \sum_1$.[12] Now it follows from (iv) that $\sum_4$ fails to meet any image of $F_3$ under powers of $T$. Hence $\rho_1 X_1(\mathfrak{U})$, since it is in $F_3 + TF_3 + \cdots T^{p-1}F_3$, must be in $M - \sum_4$. Therefore $\rho_1 X_2(\mathfrak{U})$ is a cycle mod $M - \sum_4$ of type $(\rho_1, M - \sum_4)$, and since this cycle may be assumed to be essential relative to special homologies, we conclude from (v) that $\rho_1 X_2(\mathfrak{U}) \simeq 0 \bmod M - \sum_5 + L$. Hence there exists a relation of the form

$$\rho_1 X_2(\mathfrak{U}) = \phi\rho_1 X_3(\mathfrak{U}) + \beta(\mathfrak{U}) + Z(\mathfrak{U}) \tag{1}$$

[12] For since $\rho_1(\sum_1 \cap X_2(\mathfrak{U})) = \sum_1 \cap \rho_1 X_2(\mathfrak{U}) = \rho_1 X_2(\mathfrak{U})$, we may, if necessary replace $X_2(\mathfrak{U})$ by $\sum_1 \cap X_2(\mathfrak{U})$.

where $\beta(\mathfrak{U}) \subset L$, $Z(\mathfrak{U}) \subset M - \sum_5$, $\beta(\mathfrak{U})$ and $Z(\mathfrak{U})$ having no common simplex. Since no term in (1) except $\beta(\mathfrak{U})$ contains simplexes in $L$, $\beta(\mathfrak{U}) = 0$. Hence

$$\rho_1(X_2(\mathfrak{U}) - \phi X_3(\mathfrak{U})) = 0 \bmod M - \sum_5. \tag{2}$$

Let $X_3'(\mathfrak{U}) = \sum_1 \cap X_3(\mathfrak{U})$. Since the simplexes of $X_3(\mathfrak{U})$ which are not in $\sum_1$ cannot be in $\sum_5$, we have

$$X_3(\mathfrak{U}) - X_3'(\mathfrak{U}) = 0 \bmod M - \sum_5. \tag{3}$$

Hence from (2),

$$\rho_1(X_2(\mathfrak{U}) - \phi X_3'(\mathfrak{U})) = 0 \bmod M - \sum_5. \tag{4}$$

Let $W(\mathfrak{U}) = X_2(\mathfrak{U}) - \phi X_3'(\mathfrak{U})$ and let $W'(\mathfrak{U}) = W\mathfrak{U} \cap (M - \sum_5)$. Since $W'(\mathfrak{U})$ is a subchain of $W(\mathfrak{U})$ and $W(\mathfrak{U}) \subset \sum_1$ (since $X_3'(\mathfrak{U})$ and $X_2(\mathfrak{U})$ are in $\sum_1$) we have $W'(\mathfrak{U}) \subset \sum_1$. Furthermore,

$$\rho_1(W(\mathfrak{U}) \cap (M - \sum_5)) = (\rho_1 W(\mathfrak{U})) \cap (M - \sum_5).$$

The left side is $\rho_1 W'(\mathfrak{U})$ and the right is $\rho_1 W(\mathfrak{U})$ since by (4) $\rho_1 W(\mathfrak{U}) \subset M - \sum_5$. Thus $\rho_1 W'(\mathfrak{U}) = \rho_1 W(\mathfrak{U})$ and therefore

$$\phi\rho_1 W'(\mathfrak{U}) = \phi\rho_1 W(\mathfrak{U}) = \phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U}).$$

To sum up the situation, we have now a chain $W'(\mathfrak{U})$ satisfying these conditions: $W'(\mathfrak{U}) \subset M - \sum_5$; $W'(\mathfrak{U}) \subset \sum_1$; $\phi\rho_1 W'(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U})$. By lemma 2 there exists a chain $\eta(\mathfrak{U})$ such that $\eta(\mathfrak{U}) \subset L$, $\eta(\mathfrak{U}) \subset M - \sum_5$, $\eta(\mathfrak{U}) \subset \sum_1$, and $\phi\eta(\mathfrak{U}) = \gamma(\mathfrak{U})$. Since $\mathfrak{U}$ is an arbitrary special covering we conclude by theorem A (5.1) that $\gamma \sim 0$ in $L\overline{\sum_1}(M - \sum_5)$. But $\overline{\sum_1}(M - \sum_5) = \overline{\sum_1 - \sum_5} \subset \sum_0 - \sum_5$ and hence $\gamma \sim 0$ in $L(\sum_0 - \sum_5) = L(S_0 - S_5)$.

4''. *For a given $\epsilon > 0$, there exists a $\tau < \epsilon$ such that every 1-cycle in $LF_\epsilon(a)$ is $\sim 0$ in $L(M - S_\tau)$.*

PROOF. $M_3$ has the obvious property that for every neighborhood $A(a)$, there exists an $A'(a) \subset A$ such that every cycle in $M - A$ is $\sim 0$ in $M - A'$. This property, which is similar to the property $Q$, holds also *in* $L$. (proved by an easy modification of the proof of 6.14) and 4'' follows immediately.

THEOREM 4. *Let $M$ be a euclidean 3-sphere and let $T$ be a periodic homeomorphism of $M$ with itself of prime or composite period. The set $L$ of fixed points is null or consists of two points or is a simple closed curve or is homeomorphic to an ordinary sphere.*

PROOF. Assume first that the period $q$ is a prime. As a consequence of 4.15 and 4.16, we need only consider the case in which dim $L = 2$, and this case can only arise when $q = 2$. By 7.3 $L$ is then a two-dimensional g.c.m. and hence (7.2) $L$ is a closed surface. Moreover, $L$ must be orientable since a non-orientable closed surface cannot be immersed in $M_3$. Since $L$ has the same mod 2 Betti numbers as a 2-sphere $H_2$ (4.15, 4.16) $L$ must be homeomorphic to $H_2$.

Suppose now that $q = ps$ where $p$ is a prime, and suppose moreover that $L \neq 0$. The transformation $T^s$ is of prime period $p$ and hence the totality $\mu$

is open (in $L$) and non-null, every cycle in $L'$ is $\sim 0$ in $L$. Let $\{\mathfrak{u}\}$ be the totality of finite coverings of $L$ by sets open in $L$ and let $\gamma = \{\gamma(\mathfrak{u})\}$ be a 2-cycle in $L'$. Each $\mathfrak{u}$ possesses a refinement $\mathfrak{u}_1$ of order $\leqq 3$ and since $\gamma \sim 0$, it follows that $\gamma(\mathfrak{u}_1) = 0$ for each $\mathfrak{u}_1$. Let $\pi = \pi(\mathfrak{u}_1, \mathfrak{u})$. Since $\gamma \subset L'$, we have $\gamma(\mathfrak{u}) \sim \pi\gamma(\mathfrak{u}_1)$ in $L'$, i.e. $\gamma(\mathfrak{u}) \sim 0$ in $L'$. Hence $\gamma \sim 0$ in $L'$ and 2 is verified.

3. This follows from the fact that $L$ is HLC[3] (6.15).

4. Let $S_\epsilon(a)$ denote a spherical neighborhood of radius $\epsilon$ in $M_3$ and let $F_\epsilon(a)$ be its boundary. To show that $L$ satisfies (4) it will be sufficient to verify 4′ and 4″ stated below.

4′. *Let $a$ be a point in $L$ and $\epsilon$ a number $> 0$. There exist $\delta$ and $\tau$, with $\epsilon > \delta > \tau$, such that every 0-cycle in $LF_3(a)$ is $\sim 0$ in $L(S_\epsilon(a) - S_\tau(a))$.*

Proof. Let $\sum_\epsilon(a)$ denote the invariant neighborhood $S + TS + \cdots + T^{p-1}S$ where $S = S_\epsilon(a)$. Obviously $L\sum_\epsilon(a) = LS_\epsilon(a)$. Let $\rho_3, \cdots, \rho_0$ be defined so that $\rho_3 = \sigma$.

We now choose numbers $\epsilon_0, \cdots, \epsilon_5$ such that (i) $\overline{\sum}_1 \subset \sum_0$ (where $\sum_i$, $(F_i)$ mean $\sum_{\epsilon_i}$, $(F_{\epsilon_i})$); (ii) every cycle in $\sum_2$ of type $\rho$ is $\simeq 0 \bmod L$ in $\sum_1 + L$; (iii) $F_3 \subset \sum_2$; (iv) $\sum_4 \subset S_3 \cdot TS_3 \cdots T^{p-1}S_3$; (v) every 2-cycle mod $M - \sum_4$ of type $(\rho_1, M - \sum_4)$ is $\simeq 0 \bmod M - \sum_5 + L$. The possibility of fulfilling (ii) can be readily established by methods which are by now familiar (cf. 6.5 and the proof of 6.4). The possibility of fulfilling (v) is shown as follows. From the theorem in 3.46, there can be chosen a $\sum_5 \subset \sum_4$ such that every 2-cycle mod $M - \sum_4$ of type $(\rho_2, M - \sum_4)$ is $\simeq x\Delta_2 \bmod M - \sum_5 + L$ where $\Delta_2$ is defined in 3.32. But since $\dim_\mathfrak{p} L = \dim L$ (because $M$ is a euclidean 3-sphere) and since $\dim_\mathfrak{p} = r(\mathfrak{p})$ (4.11) we conclude that $r(\mathfrak{p}) = 2$ and hence (3.48) $\Delta_2 \simeq 0 \bmod M - \sum_5 + L$.—We shall show that for $\delta$, $\tau$ in condition 4′ we may take $\epsilon_0$, $\epsilon_5$. For this we must show that if $\gamma_0$ is a 0-cycle in $LF_3$, then $\gamma_0 \sim 0$ in $L(S_0 - S_5)$.

Since $\gamma_0 \subset F_3$ and $F_3$ is homeomorphic to an ordinary sphere, $\gamma_0 \sim 0$ in $F_3$. Thus we may write $\gamma_0 = \phi X_1$, $X_1 \subset F_3$. Hence $\rho_1 X_1(\mathfrak{U})$ is a cycle of type $\rho_1$ and by (iii) $\rho_1 X_1(\mathfrak{U}) \subset \sum_2$. We may assume that $\rho_1 X_1(\mathfrak{U})$ is essential relative to special homologies and hence by (ii) $\rho_1 X_1(\mathfrak{U}) \simeq 0 \bmod L$ in $\sum_1 + L$. Thus there exists a relation of the form $\phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U}) + \alpha(\mathfrak{U})$ where $\rho_1 X_2(\mathfrak{U}) \subset \sum_1 + L$, $\alpha(\mathfrak{U}) \subset L$. Since $L \cap \rho_1 X_2(\mathfrak{U}) = 0$, we have $\rho_1 X_2(\mathfrak{U}) \subset \sum_1$. Since also $L \cap \rho_1 X_1(\mathfrak{U}) = 0$, we have $\alpha(\mathfrak{U}) = 0$, and therefore $\phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U})$. In this relation, *we may assume that* $X_2(\mathfrak{U}) \subset \sum_1$.[12] Now it follows from (iv) that $\sum_4$ fails to meet any image of $F_3$ under powers of $T$. Hence $\rho_1 X_1(\mathfrak{U})$, since it is in $F_3 + TF_3 + \cdots T^{p-1}F_3$, must be in $M - \sum_4$. Therefore $\rho_1 X_2(\mathfrak{U})$ is a cycle mod $M - \sum_4$ of type $(\rho_1, M - \sum_4)$, and since this cycle may be assumed to be essential relative to special homologies, we conclude from (v) that $\rho_1 X_2(\mathfrak{U}) \simeq 0 \bmod M - \sum_5 + L$. Hence there exists a relation of the form

$$\rho_1 X_2(\mathfrak{U}) = \phi\rho_1 X_3(\mathfrak{U}) + \beta(\mathfrak{U}) + Z(\mathfrak{U}) \tag{1}$$

[12] For since $\rho_1(\sum_1 \cap X_2(\mathfrak{U})) = \sum_1 \cap \rho_1 X_2(\mathfrak{U}) = \rho_1 X_2(\mathfrak{U})$, we may, if necessary replace $X_2(\mathfrak{U})$ by $\sum_1 \cap X_2(\mathfrak{U})$.

where $\beta(\mathfrak{U}) \subset L$, $Z(\mathfrak{U}) \subset M - \sum_5$, $\beta(\mathfrak{U})$ and $Z(\mathfrak{U})$ having no common simplex. Since no term in (1) except $\beta(\mathfrak{U})$ contains simplexes in $L$, $\beta(\mathfrak{U}) = 0$. Hence

$$\rho_1(X_2(\mathfrak{U}) - \phi X_3(\mathfrak{U})) = 0 \bmod M - \sum_5. \tag{2}$$

Let $X_3'(\mathfrak{U}) = \sum_1 \cap X_3(\mathfrak{U})$. Since the simplexes of $X_3(\mathfrak{U})$ which are not in $\sum_1$ cannot be in $\sum_5$, we have

$$X_3(\mathfrak{U}) - X_3'(\mathfrak{U}) = 0 \bmod M - \sum_5. \tag{3}$$

Hence from (2),

$$\rho_1(X_2(\mathfrak{U}) - \phi X_3'(\mathfrak{U})) = 0 \bmod M - \sum_5. \tag{4}$$

Let $W(\mathfrak{U}) = X_2(\mathfrak{U}) - \phi X_3'(\mathfrak{U})$ and let $W'(\mathfrak{U}) = W\mathfrak{U} \cap (M - \sum_5)$. Since $W'(\mathfrak{U})$ is a subchain of $W(\mathfrak{U})$ and $W(\mathfrak{U}) \subset \sum_1$ (since $X_3'(\mathfrak{U})$ and $X_2(\mathfrak{U})$ are in $\sum_1$) we have $W'(\mathfrak{U}) \subset \sum_1$. Furthermore,

$$\rho_1(W(\mathfrak{U}) \cap (M - \sum_5)) = (\rho_1 W(\mathfrak{U})) \cap (M - \sum_5).$$

The left side is $\rho_1 W'(\mathfrak{U})$ and the right is $\rho_1 W(\mathfrak{U})$ since by (4) $\rho_1 W(\mathfrak{U}) \subset M - \sum_5$. Thus $\rho_1 W'(\mathfrak{U}) = \rho_1 W(\mathfrak{U})$ and therefore

$$\phi\rho_1 W'(\mathfrak{U}) = \phi\rho_1 W(\mathfrak{U}) = \phi\rho_1 X_2(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U}).$$

To sum up the situation, we have now a chain $W'(\mathfrak{U})$ satisfying these conditions: $W'(\mathfrak{U}) \subset M - \sum_5$; $W'(\mathfrak{U}) \subset \sum_1$; $\phi\rho_1 W'(\mathfrak{U}) = \rho_1 X_1(\mathfrak{U})$. By lemma 2 there exists a chain $\eta(\mathfrak{U})$ such that $\eta(\mathfrak{U}) \subset L$, $\eta(\mathfrak{U}) \subset M - \sum_5$, $\eta(\mathfrak{U}) \subset \sum_1$, and $\phi\eta(\mathfrak{U}) = \gamma(\mathfrak{U})$. Since $\mathfrak{U}$ is an arbitrary special covering we conclude by theorem A (5.1) that $\gamma \sim 0$ in $L\overline{\sum_1}(M - \sum_5)$. But $\overline{\sum_1}(M - \sum_5) = \overline{\sum_1 - \sum_5} \subset \sum_0 - \sum_5$ and hence $\gamma \sim 0$ in $L(\sum_0 - \sum_5) = L(S_0 - S_5)$.

4''. *For a given $\epsilon > 0$, there exists a $\tau < \epsilon$ such that every 1-cycle in $LF_\epsilon(a)$ is $\sim 0$ in $L(M - S_\tau)$.*

PROOF. $M_3$ has the obvious property that for every neighborhood $A(a)$, there exists an $A'(a) \subset A$ such that every cycle in $M - A$ is $\sim 0$ in $M - A'$. This property, which is similar to the property $Q$, holds also *in* $L$. (proved by an easy modification of the proof of 6.14) and 4'' follows immediately.

THEOREM 4. *Let $M$ be a euclidean 3-sphere and let $T$ be a periodic homeomorphism of $M$ with itself of prime or composite period. The set $L$ of fixed points is null or consists of two points or is a simple closed curve or is homeomorphic to an ordinary sphere.*

PROOF. Assume first that the period $q$ is a prime. As a consequence of 4.15 and 4.16, we need only consider the case in which dim $L = 2$, and this case can only arise when $q = 2$. By 7.3 $L$ is then a two-dimensional g.c.m. and hence (7.2) $L$ is a closed surface. Moreover, $L$ must be orientable since a non-orientable closed surface cannot be immersed in $M_3$. Since $L$ has the same mod 2 Betti numbers as a 2-sphere $H_2$ (4.15, 4.16) $L$ must be homeomorphic to $H_2$.

Suppose now that $q = ps$ where $p$ is a prime, and suppose moreover that $L \neq 0$. The transformation $T^s$ is of prime period $p$ and hence the totality $\mu$

of its fixed points is one of the sets mentioned in the theorem. $T$ induces a transformation $T_1$ of $\mu$ into itself (see proof of theorem 3) and since $T_1^q$ is the identity (in $\mu$) $T_1$ is the identity or else is periodic. The set $L_1$ of points of $\mu$ which are invariant under $T_1$ is identical with $L$ (cf. proof of theorem 3). If $T_1$ is the identity then $L = \mu$ and the theorem is established. Suppose $T_1$ is not the identity. $\mu$ cannot be null for then $L$ would be null; nor can $\mu$ consist of two points for then either $T_1$ is the identity or else $L_1 = L = 0$. Suppose $\mu$ is a simple close curve or is homeomorphic to $H_2$. That $L_1$ (hence $L$) is one of the sets in question can be proved readily by the methods we have developed, or follows from the remark that that every periodic homeomorphic transformation of a circle or sphere into itself is topologically equivalent to an orthogonal transformation.[13]

REMARK. If we keep in mind the method of passing from prime periods for $T$ to composite periods, it will be readily seen from a glance at 4.15, 4.16 that the different types of fixed-point sets in theorem 4 can arise in the following ways:

*If $T$ preserves orientation in $M_3$, $L$ is either null or a simple closed curve. If $T$ reverses orientation, either $L$ is homeomorphic to $H_2$ and $T$ is of period 2 or else $L$ consists of two points and the period of $T$ is even.*

**8.1.** *Orientability.* We have asserted elsewhere without proof (see introduction) that if the space $M$ is orientable and if the period $p$ of $T$ is odd then, at least in the analytic case, the components of $L$ are themselves orientable. We shall now prove this for a case somewhat more general than the analytic one. We begin by studying the $r^{\text{th}}$ Betti number of a component of type $P_rQ$.

Let $M$ be a connected space of type $P_mQ$ and dimension $m$. We shall say that $M$ is an $m$-dimensional *quasi-manifold* if there exists a cycle $\Gamma_m$ which is a homology basis for $m$-cycles and is such that for every point $d$ of $M$ there is a fundamental pair of the form $(D(d), \Gamma_m)$.

*Let $M$ be an $m$-dimensional space of type $P_mQ$ such that $B_m(M) = 1$ and such that all $m$-cycles in an arbitrary closed proper subset of $M$ are $\sim 0$. Then $M$ is a quasi-manifold.*

PROOF. Let $\Gamma_m$ be a homology basis for $m$-cycles and let $C$ be a non-null open set in $M$. *Then $\Gamma_m$ is not $\sim 0$ mod $M - C$.* For let $\Gamma' = \Gamma \cap (M - C)$ and $\Gamma'' = \Gamma - \Gamma'$. Then $\Gamma'' = \Gamma \bmod M - C$. Hence if $\Gamma \sim 0 \bmod M - C$, we have also $\Gamma'' \sim 0 \bmod M - C$, say $\phi X_{m+1} = \Gamma'' + \gamma$ where $\gamma \subset M - C$. Now $\phi(\Gamma' - \gamma) = -\phi(\Gamma'' + \gamma) = -\phi\phi X = 0$ so that for each $\mathfrak{U}$, $\Gamma'(\mathfrak{U}) - \gamma(\mathfrak{U})$ is a cycle. We may assume that this cycle is essential (see proof of 6.4). Then since $\Gamma'(\mathfrak{U}) - \gamma(\mathfrak{U})$ is in the non-null closed set $M - C$, we have $\Gamma'(\mathfrak{U}) - \gamma(\mathfrak{U}) \sim 0$. But since $\Gamma''(\mathfrak{U}) + \gamma(\mathfrak{U}) \sim 0$ it follows that $\Gamma = \Gamma' + \Gamma'' \sim 0$ which is impossible.—Now consider the fundamental pair $(D(d), {}^d\Omega_m)$ for $d$ which exists since $M$ is of type $P_mQ$. Suppose $B(b) \subset D$. Then there exists a $B'(b) \subset B$ such that $\Gamma_m \sim x\Omega_m \bmod M - B'$ (by property $P_m$) and from what we have

[13] For the case of spheres see Brouwer [12] and Kerékjártó [13]; for circles, see J. F. Ritt, *On certain real solutions of Babbage's functional equation*, Annals of Math., 17 (1915) 113-122.

just proved, we conclude that $x \neq 0$. Hence $\Gamma$, as well as $\Omega$, constitutes a basis for $m$-cycles mod $M - B$ relative to homologies mod $M - B'$ and $(D, \Gamma)$ is therefore a fundamental pair for $d$.

On the basis of the preceding theorem it can be shown without great difficulty that, for example, every absolute manifold mod $p$ (Lefschetz, *Topology*, p. 120) is a quasi-manifold relative to $\mathfrak{p}$ and every compact locally euclidean space is a quasi-manifold relative to every $\mathfrak{f}$.

THEOREM 5. *Let $M$ be a quasi-manifold which is* HLC$^m$ *and let $T$ be a periodic homeomorphism of $M$ with itself, of prime period $p$. Let $L_1, \cdots, L_l$ be the components of the set $L$ of fixed points, $L_i$ being of type $P_{r_i}Q$ (theorem 3). Then $B_{r_i}(L_i) \geqq 1$.*

PROOF. Let $\Gamma_m$ be a homology basis for $m$-cycles, such that every point $d$ has a fundamental pair of the form $(D(d), \Gamma_m)$. Since $\dim M = m$, it follows from 3.31 that $\Gamma_m$ is a cycle of type $(\rho_m, L)(\rho_m = \sigma)$. Let $\Gamma_m$ now be denoted by $\Delta_m$.

Let $d$ be a point of $L$ and $E(d)$ an invariant neighborhood of $d$ such that $E(d) \subset D(d)$. Suppose $\Delta_m \simeq 0 \bmod M - E' + L$ where $E'$ is a non-null open invariant subset of $E$. Then $\Delta_m = 0 \bmod M - E' + L$ (3.31). Since $L$ is nowhere dense in $M$, there exists a non-null open subset $B$ of $E'$ such that $BL = 0$. Then $\Delta = 0 \bmod M - B$ which is impossible. We conclude that $\Delta$ is not $\simeq 0 \bmod M - E' + L$ and therefore $(E(d), \Delta_m)$ is a *special* fundamental pair (6.5).

Let us form the sequence $\Delta_m, \cdots, \Delta_0$ of 3.32 (with $m$ now in place of $n$). We may write

$$\Delta_h = \rho_h\chi_h + \gamma_h, \qquad \gamma_h \subset L \qquad (h = m, \cdots, 0)$$

$$\phi\chi_h = \Delta_{h-1}. \qquad (h = m, \cdots, 1)$$

We assert that if $h \leqq m - 1$, $\gamma_h$ *is a cycle in* $L$. For consider the mapping $\Lambda$ of $M$ into the modular space $M^*$ (see 2.2 and 3.1). Then by 3.19, $\Lambda\chi_{h+1}$ is a cycle mod $L^*$ in $M^*$ and by 1.2 $\phi\Lambda\chi_{h+1}$ is therefore a cycle in $L^*$. Since $\phi\Lambda\chi_{h+1} = \Lambda\phi\chi_{h+1} = \Lambda(\rho_h\chi_h + \gamma_h)$ and since $\Lambda\rho_h\chi_h = 0$, it follows that $\phi\Lambda\chi_{h+1} = \Lambda\gamma_h =$ a cycle in $L^*$. $\Lambda$, however, induces a homeomorphism between $L$ and $L^*$ and therefore $\gamma_h$ is a cycle in $L$.

Suppose now that $d$ is in the component $L_1$ say. We recall that $\Delta_{r_1}$ is the first cycle in the sequence $\Delta_m, \cdots, \Delta_0$, which is $\simeq 0 \bmod M - F + L$ where $F$ is defined in 6.10. We now assert that if $F'$ is an invariant open subset of $F$ such that $LF' \neq 0$, $\gamma_r$ $(r = r_1)$ is not $\sim 0 \bmod L(M - F')$ in $L$. For suppose on the contrary that $\gamma_r = \phi\zeta_{r+1} - \eta_r$ where $\zeta \subset L$ and $\eta \subset L(M - F')$. The relation $\Delta_r \simeq 0 \bmod M - F + L$ holds also mod $M - F' + L$ and hence there exists a relation of the form

$$\phi\rho_r H_{r+1} = \rho_r\chi_r + \gamma_r + \beta_r + K_r$$

where $\beta_r \subset L$, $K_r \subset M - F'$, and where $\beta$ and $K$ have no common complex. Evidently $K_r$ must be of the form $\rho_r J$ where $J \subset M - F'$. Since

$(\rho_r(\phi H - \chi_r - J)) \cap L = 0$ and $\beta + \gamma \subset L$, we must have $\phi\rho_r H = \rho_r\chi_r + \rho_r J$. Let

$$Z_{r+1} = \chi_{r+1} - \rho_r H_{r+1} - \zeta_{r+1}.$$

Then $\phi Z_{r+1} = -\rho_r J - \eta \subset M - F'$. Thus each $Z_{r+1}(\mathfrak{U})$ is a cycle mod $M - F'$. We may by the usual argument assume that any given $Z_{r+1}(\mathfrak{U})$ is essential. Since $r \leqq m - 1$ (6.10) there exists an open invariant $F'' \subset F'$ $(F'' \neq 0)$ such that $Z_{r+1}(\mathfrak{U}) \sim 0 \bmod M - F''$. From 6.4 there exists an open invariant $F''' \subset F''$ $(F''' \neq 0)$ such that $\rho_{r+1}Z_{r+1} \simeq 0 \bmod M - F''' + L$. But $\rho_{r+1}Z_{r+1} = \rho_{r+1}\chi_{r+1} = \Delta_{r+1}$. Thus $\Delta_{r+1} \simeq 0 \bmod M - F''' + L$ which is impossible. This establishes our assertion that $\gamma_r$ is not $\sim 0 \bmod L(M - F')$ in $L$. It follows *a fortiori* that $\gamma_r$ is not $\sim 0$ in $L$. Now let $\gamma' = L_1 \cap \gamma$. Since $L$ has only a finite number of components, it is quite easy to see that $\gamma'$ is a cycle in $L_1$. Suppose that $F'$ were chosen so small that $F'(L - L_1) = 0$. If $\gamma' \sim 0$ in $L_1$, then also

$$\gamma' \sim 0 \bmod L(M - F') \text{ in } L. \tag{1}$$

Since $\gamma - \gamma' \subset L - L_1 \subset L(M - F')$, so that $\gamma - \gamma' = 0 \sim 0 \bmod L(M - F')$ in $L$, we have, on adding this last relation to (1), $\gamma \sim 0 \bmod L(M - F')$ in $L$. Since this is impossible, we conclude that $\gamma_r$ is not $\sim 0$ in $L_1$. Hence $B_{r_1}(L_1) \geqq 1$.

**8.2.** Let $M_m$ be a connected locally euclidean space of $m$ dimensions and $T$ a periodic homeomorphism of $M_m$ with itself. If the fixed-point set for $T$ as well as every power of $T$ is locally euclidean, we shall call $T$ *regular*. If for example $T$ is locally analytic then it is regular.

THEOREM 6. *Let $T$ be a regular periodic homeomorphism of a connected compact locally euclidean space $M_m$ with itself. If $M_m$ is orientable and if the period of $T$ is odd, then every component of the set $L$ of fixed points is orientable.*

PROOF. Suppose first that the period $q$ is an odd prime. From the theory of locally euclidean spaces,[14] $B_m(M_m; \mathfrak{q}) = 1$ or 0 according as $M_m$ is orientable or not. Assume now that $M_m$ is orientable. Then $B_m(M_m; \mathfrak{q}) = 1$ and it follows from theorem 5 that $B_{r_i}(L_i; \mathfrak{q}) \geqq 1$ where $L_i$ is a component of $L$ of type $P_{r_i}Q$. Since $L_i$ is locally euclidean, $\dim_{\mathfrak{q}} L_i = \dim L_i$ and hence $\dim L = r_i$. It follows that $B_{r_i}(L_i) = 1$ and $L_i$ is orientable.

Suppose now that $q = ps$ where $p$ is an odd prime and $s$ is odd. We shall prove the theorem by induction on $m$. For $m = 1$, the theorem is true since $M$ is then a simple closed curve and $L$ consists of two points. Suppose the theorem is true for dimensions $m - 1$. The transformation $T^s$ is of prime period $p$ and therefore its fixed-point set $\mu$ consists of a finite number of orientable locally euclidean spaces, and by theorem 2 each component is of dimension $\leqq m - 1$. As shown in the proof of theorem 3, each component of $\mu$

[14] See W. W. Flexner, *On topological manifolds*, Ann. of Math. 32 (1931), pp. 393–406; *The Poincaré duality theorems for topological manifolds*, Ann. of Math. 32 (1931), pp. 539–548.

which contains points of $L$ is transformed by $T$ into itself. Let $T_i$ be the transformation induced by $T$ in $\mu_i$ ($\mu_i L \neq 0$) and let $L_i$ be the set of points in $\mu_i$ left invariant by $T_i$. Then $L = \sum L_i$. Since $T_i^{\sigma}$ is the identity, $T_i$ is either periodic or is the identity. If $T_i$ is the identity, $\mu_i = L_i$ so that $L_i$ is orientable. If $T_i$ is periodic it follows from the hypothesis of the induction that the components of each $L_i$ are orientable; hence those of $L$ are orientable.

## Corrections and Comments

In connection with Transformations of finite period, these Annals 39 (1938), pp. 127–164).

Page 143, line 1, replace $B$ by $L$.

Page 143: in connection with the proof of 3.15, the remarks in 6.0 of the present paper will be helpful.

Page 149: section 3.35 should be replaced by the statement and proof of lemma 1 in the present paper. This will necessitate minor changes in the proofs of 3.36 and 3.49. But 3.36 and 3.49 are essentially special cases of theorem 3 and section 6.10 respectively in the present paper.

Page 153, line 14, omit $(a \subset L)$; line 18, replace $n - 2$ by $n - 1$; line 22, after the period insert the sentence "For $h = n - 1$ we must use an obvious modification of 3.39 for relative cycles."

Page 155, line 21, replace $\pi_2$ by $\pi_1$.

Page 155, line 22, insert $X_{r+1}$ after $\rho_{r+1}$.

Page 156, lines 18, 19, 21, replace $\rho_n$ by $\rho_{n-1}$.

Page 158, next to last line, change 3.23 to 3.22.

Page 162, line 19, replace $T$ by $T^q$.

Barnard College,
Columbia University.

ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

# RINGS WITH MINIMAL CONDITION FOR LEFT IDEALS

BY CHARLES HOPKINS

(Received December 9, 1938)

## INTRODUCTION

One finds in the literature a thorough-going discussion of rings without radical and with minimal condition for left ideals (semi-simple rings). For the structure of a ring whose quotient-ring with respect to the radical is semi-simple one can refer to the investigations of Köthe (see $K$ below). In this paper we shall examine the structure of a ring $A$ with radical $R \supset 0$ and with minimal condition for left ideals ("general" MLI ring).

The key-stone of our investigations is the fact that the radical of $A$ is nilpotent, and this result we shall establish in §1. In §2 we shall prove that the sum of all minimal non-zero left ideals is a completely-reducible left ideal $\mathfrak{M}$, and in §3 we shall examine the distribution of idempotent and nilpotent left ideals in $\mathfrak{M}$.

In §§4–6 we shall discuss the two "extreme cases": (1) when $A$ is nilpotent, and (2) when $A$ is idempotent. For a non-nilpotent $A$ we shall prove that the existence of either a right-hand or a left-hand identity is sufficient for the existence of a composition series of left ideals of $A$. If $A$ is any MLI ring, one can find a smallest exponent $k$ such that $A^k = A^{k+1} = \cdots$. In §7 we show that $A$ is the sum of $A^k$ (which is idempotent) and a nilpotent MLI ring.

We wish to emphasize the fact that $A$ is to be regarded throughout as a *ring without operators*. In §8, however, we shall see that some of our most interesting results are valid for operator domains of a certain type.

We conclude the Introduction with an explanation of our notation and terminology. Rings and subrings will usually be denoted by roman capitals; we shall use gothic letters when it is desirable to emphasize the fact that a subring is an ideal. By the statement "$\mathfrak{a}$ is a left (right) ideal of $A$" we shall mean that $\mathfrak{a}$ is an additive abelian group which admits the elements of $A$ as left-hand (right-hand) operators. Observe that our definition does not[1] imply that $\mathfrak{a}$ is a subring of $A$. The term "left ideal," with no qualifying phrase, will always mean "left ideal of the basic ring." A ring with minimal condition for left (right) ideals which are contained in itself will be called an MLI (MRI) ring. Finally we point out that if $\mathbf{a}$ and $\mathbf{b}$ are subrings of $A$, then $[\mathbf{a}, \mathbf{b}]$ denotes the cross-cut of $\mathbf{a}$ and $\mathbf{b}$, while $(\mathbf{a}, \mathbf{b})$ represents the compound (join) of $\mathbf{a}$ and $\mathbf{b}$—i.e.

[1] One might object to this extension on the ground that an adequate terminology is already available. But we prefer the compact description "$\mathfrak{a}$ is a two-sided ideal of $A$" to its cumbersome equivalent: "$\mathfrak{a}$ is a ring (not necessarily contained in $A$) which admits the elements of $A$ as left-hand and right-hand operators."

the cross-cut of all subrings of $A$ containing both $\mathfrak{a}$ and $\mathfrak{b}$. For homomorphism and isomorphism we shall use the symbols $\sim$ and $\cong$ respectively.

Whenever possible, references will be made to standard treatises rather than to original sources. In the list below the symbol in parentheses is the abbreviation we shall use in the footnotes.

L. E. DICKSON, *Algebras and their Arithmetics* (D1)

L. E. DICKSON, *Algebren und ihre Zahlentheorie* (D2)

M. DEURING, *Algebren*, Ergebnisse IV, I (D)

G. KÖTHE, *Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist*, Math. Z. Vol. 32 (1930), pp. 161–186 (K)

W. KRULL, *Über verallgemeinerte Abelsche Gruppen*, Math. Z. Vol. 23 (1925), pp. 161–186 (Kr.)

B. L. VAN DER WAERDEN, *Moderne Algebra*, Vol. II (v.d.W. II).

**1.** Let $A$ be any MLI ring and let $R$ denote its radical. Throughout this section we shall assume $R \supset 0$, although our results are trivially true for $R = 0$. Now the term *radical* of a non-commutative ring has been variously defined.[2] From the results of this section it will be clear that for an MLI ring the three definitions referred to in the footnote are all equivalent. These definitions agree on the following properties of $R$: (a) *$R$ is a two-sided ideal of $A$*; (b) *$R$ contains every nilpotent left ideal of $A$*; (c) *every element of $R$ is nilpotent*; and since it is exactly these properties which we shall need, we may choose any one of these three definitions for $R$. For the sake of explicitness, however, let us adopt the definition in v.d.W. II.

Our principal objective in this section is to show that $R$ is nilpotent. For the proof we shall require the lemmas 1.1, 1.2, 1.3 below.

1.1: *If $\mathfrak{l}$ is any minimal non-zero left ideal of a ring $T$, and if $\mathfrak{n}$ is any left nilideal of $T$, then $\mathfrak{n}\mathfrak{l} = 0$.*

PROOF: Since $\mathfrak{l}$ is minimal and since $\mathfrak{n}\mathfrak{l}$ is a left ideal of $T$, we have only to prove that $\mathfrak{n}\mathfrak{l} \neq \mathfrak{l}$; for we must have either $\mathfrak{n}\mathfrak{l} = \mathfrak{l}$ or $\mathfrak{n}\mathfrak{l} = 0$. Suppose that $\mathfrak{n}\mathfrak{l} = \mathfrak{l}$; then for some non-zero element $u$ of $\mathfrak{l}$ we must have $\mathfrak{n}u = \mathfrak{l}$, since $\mathfrak{n}u$ is itself a left ideal of $T$ contained in the minimal left ideal $\mathfrak{l}$. But if $\mathfrak{n}u = \mathfrak{l}$, then $\mathfrak{n}$ must contain an element $b$ such that $bu = u$. Since $\mathfrak{n}$ is a nilideal—i.e. an ideal containing only nilpotent elements—we should then have $u = bu = b^2u = \cdots = 0$, contrary to the assumption $u \neq 0$. Hence $\mathfrak{n}\mathfrak{l} = 0$, since we have eliminated the alternative $\mathfrak{n}\mathfrak{l} = \mathfrak{l}$.

1.2: *If $A$ is an* MLI *ring with radical $R \supset 0$, then the right annihilator $N_1$ of $R$ in $R$ is a non-zero two-sided ideal of $A$.*

PROOF: By the term *right annihilator of $R$ in $R$* we mean the set $N_1$ of all elements $x$ in $R$ for which $Rx = 0$. Since $R$ is a left ideal of the MLI ring $A$,

[2] One finds in the literature the following definitions for the radical of a ring $T$: "the set of all properly nilpotent elements of $T$," *D2*, p. 97; "the maximal two-sided nilideal $R$ of $T$, provided that $R$ contains all one-sided nilideals of $T$," *D*, p. 11—also *K*, p. 168; "the set of all elements $x$ such that $x$ generates a nilpotent two-sided ideal," V.d.W. II, p. 155.

it must contain at least one minimal non-zero left ideal $\mathfrak{l}$, and from Lemma 1.1 we know that $R\mathfrak{l} = 0$. Hence $N_1 \supset 0$, since it contains at least the elements of $\mathfrak{l}$.

From the associative law of multiplication in $A$ we have $R(N_1A) = (RN_1)A = 0$. Hence $N_1$ is a right ideal of $A$. Since the radical $R$ is a right ideal of $A$ we have $R(AN_1) = (RA)N_1 \subseteq RN_1 = 0$. Hence $N_1$ is also a left ideal of $A$.

1.3: *If* $\mathfrak{s}_1, \mathfrak{s}_2, \cdots \mathfrak{s}_n$ *are any* $n$ *subrings of a ring* $T$, *and if the symbol* $\mathfrak{s}:t$ *be defined as the set of all elements* $x$ *in* $T$ *for which* $tx$ *is contained in* $\mathfrak{s}$, *then* $(\cdots(\mathfrak{s}_1:\mathfrak{s}_2):\mathfrak{s}_3\cdots):\mathfrak{s}_n = \mathfrak{s}_1:\mathfrak{s}_2\mathfrak{s}_3\cdots\mathfrak{s}_n$.

Proof: Let $x$ be any element of $\mathfrak{s}_1:\mathfrak{s}_2\mathfrak{s}_3$. Then $\mathfrak{s}_2\mathfrak{s}_3x$ is in $\mathfrak{s}_1$. Since $\mathfrak{s}_2\mathfrak{s}_3x = \mathfrak{s}_2(\mathfrak{s}_3x)$, we see that $\mathfrak{s}_3x$ is in $\mathfrak{s}_1:\mathfrak{s}_2$. So we have $\mathfrak{s}_1:\mathfrak{s}_2\mathfrak{s}_3 \subseteq (\mathfrak{s}_1:\mathfrak{s}_2):\mathfrak{s}_3$.

Let $y$ be any element of $(\mathfrak{s}_1:\mathfrak{s}_2):\mathfrak{s}_3$. Then $\mathfrak{s}_3y$ is in $\mathfrak{s}_1:\mathfrak{s}_2$, which implies that $\mathfrak{s}_2\mathfrak{s}_3y$ is in $\mathfrak{s}_1$. From this follows $(\mathfrak{s}_1:\mathfrak{s}_2):\mathfrak{s}_3 \subseteq \mathfrak{s}_1:\mathfrak{s}_2\mathfrak{s}_3$. Hence $(\mathfrak{s}_1:\mathfrak{s}_2):\mathfrak{s}_3 = \mathfrak{s}_1:\mathfrak{s}_2\mathfrak{s}_3$, and one can easily complete the proof by induction.

We are now in a position to establish our main theorem:

1.4: *The radical of an* MLI *ring is nilpotent.*

Proof: Let $A$ be an MLI ring with radical $R \supset 0$. From 1.2 we know that the right annihilator $N_1$ of $R$ in $R$ is a non-zero two-sided ideal. If $N_1 = R$, then $R^2 = RN_1 = 0$, and our theorem is valid. So we assume $N_1 \subset R$ and construct the quotient-rings $A' = A/N_1$ and $R' = R/N_1$. Now $A'$ is an MLI ring[3] with radical $R' \supset 0'$. From 1.2 we know that $R'$ contains a right annihilator $N_2' \supset 0'$ which is a two-sided ideal of $A'$. Let $N_2$ denote the homomorphic[4] image of $N_2'$ in $A$ under the homomorphism $A \sim A'$. Since $N_2' \supset 0'$ we have $N_2 \supset N_1$.

Suppose that $N_i'$ and $N_i$ have already been defined for $i < j$. Then we define $N_j'$ to the right annihilator of $R/N_{j-1}$ in $R/N_{j-1}$ and $N_j$ to be the homomorphic image of $N_j'$ in $A$.

Consider the ascending chain

(1) $N_1 \subseteq N_2 \subseteq \cdots$. By definition, $N_i' = 0:(R/N_{i-1})$ and $N_i = N_{i-1}:R$. From 1.3 we have $N_{i-1}:R = (\cdots((0:R):R)\cdots)R = 0:R^i$. Hence $N_i = 0:R^i$.

Consider the descending chain

(2) $R \supseteq R^2 \supseteq \cdots$. Each term in (2) is a left ideal of $A$, and since $A$ is an MLI ring[5] we must have the equality sign in (2) after a finite number of terms. Let $k$ be the smallest exponent for which $R^k = R^{k+1} = \cdots$.

Now $N_k \subset R$ requires $N_{k+1}' \supset 0$ and $N_{k+1} \supset N_k$. But $N_k = 0:R^k$ and

---

[3] Every quotient-ring of an MLI ring is an MLI ring, see Kr., p. 170.

[4] In general there are an infinite number of distinct homomorphisms of $A$ with $A/\mathfrak{a}$, where $\mathfrak{a}$ is a two-sided ideal. We tacitly assume, however, that $A \sim A'$ refers only to the homomorphism defined by the correspondence $x \to x + \mathfrak{a}$, $x$ arbitrary in $A$. It is obvious that this correspondence defines not only a ring-homomorphism but also an operator-homomorphism with respect to the elements of A as both left-hand and right-hand operators.

[5] It is well known that the minimal condition for left (right) ideals is equivalent to the descending chain condition for left (right) ideals.

$N_{k+1} = 0{:}R^{k+1}$; and since $R^k = R^{k+1}$ we must have $N_k = N_{k+1}$. It follows, then, that $N_k$ is equal to $R$.

From $N_k = R$ we have $R^{k+1} = R^k N_k = 0$; that is, $R$ is nilpotent and of exponent $\rho = k + 1$. This completes the proof of 1.4.

We shall define the *left annihilator* $M_1$ *of* $R$ *in* $R$ to be the set of all elements $x$ in $R$ for which $xR = 0$. From the fact that $R$ is nilpotent and of exponent $\rho = k + 1$ it is not difficult to establish the following result.

1.5: *Let* $A$ *be an* MLI *ring with radical* $R \supset 0$. *If* $M_i$ *be defined as the left annihilator of* $R^i$ *in* $R$, *then* $M_i \subset M_{i+1}$ *for* $i \leqq \rho - 2$; $M_{\rho-1} = R$, *where* $\rho$ *is the exponent of* $R$; *and each* $M_i$ *is a two-sided ideal of* $A$.

Proof: That $M_i$ is not zero for $i \geqq 1$ follows from the fact that $M_i$ contains $R^{\rho-i}$, which is not zero. But $M_{i-1}$ does not contain $R^{\rho-i}$; if it did, we should have $R^{\rho-i} \cdot R^{i-1} \subsetneq M_{i-1} \cdot R^{i-1} = 0$, whereas $R^{\rho-i} \cdot R^{i-1} = R^{\rho-1} \neq 0$. This proves that $M_{i-1}$ is contained properly in $M_i$. Obviously $M_{\rho-1} \supseteqq R$, since $R \cdot R^{\rho-1} = 0$. By definition, each $M_i$ is contained in $R$. Hence $M_{\rho-1} = R$.

Evidently $M_i$ is a left ideal. From the relations $(M_iA)R^i = M_i(AR^i) \subseteq M_iR^i = 0$, it is equally evident that $M_i$ is a right ideal of $A$.

As a final remark in connection with 1.5 we point out that $M_{i+1}/M_i$ is the left annihilator of $R/M_i$ in $R/M_i$—i.e. $M_{i+1}R \subseteq M_i$.

We conclude this section by stating two corollaries of 1.4 which we shall need in what follows.

1.6: *An* MLI *ring is semi-primary.*[6]

1.7: *In an* MLI *ring any subring containing only nilpotent elements is itself nilpotent.*

**2.** Evidently an MLI ring $A$ contains at least one minimal non-zero left ideal. The main result of this section is the following theorem:

2.1: *If* $A$ *is an* MLI *ring, then the sum*[7] $\mathfrak{M}$ *of all minimal non-zero left ideals of* $A$ *is* (i) *a two-sided ideal of* $A$ *and* (ii) *the direct sum of a finite number of minimal non-zero left ideals.*

We shall need the following lemmas, the proofs of which are given in v.d.W. II, p. 157.

($\alpha$) *If* $\mathfrak{L}$ *is a left ideal of a ring* $T$, $c$ *any element of* $T$, *then the correspondence* $x \to xc$, *for variable* $x$ *in* $\mathfrak{L}$, *defines a homomorphism of the modulus* $\mathfrak{L}$ *with the modulus* $\mathfrak{L}c$, *and this homomorphism is an operator-homomorphism with respect to the elements of* $T$ *as left-hand operators.*

($\beta$) *If* $\mathfrak{l}$ *is a minimal left ideal of* $T$, *and if* $\mathfrak{l} \sim \mathfrak{l}'$ *is an operator-homomorphism (with respect to left-hand multiplication by elements of* $T$), *then either* $\mathfrak{l}' = 0$ *or* $\mathfrak{l} \cong \mathfrak{l}'$.

---

[6] A ring $T$ is called semi-primary if the quotient-ring with respect to the radical of $T$ is semi-simple (D, p. 13). Proofs of 1.6 and 1.7 are given in the article entitled "Nilrings with Minimal Condition for Admissible Left Ideals," Duke Mathematical Journal, vol. 4 (1938), p. 667.

[7] By the term "sum" of the left ideals $\mathfrak{a}$, $\mathfrak{b}$, $\cdots$ we mean the set of all sums $a + b + \cdots + n$, $a \in \mathfrak{a}$ etc. for which only a finite number of components are different from zero.

($\gamma$) *If* $\mathfrak{l}$ *is a minimal non-zero left ideal of* $T$, *then either* $\mathfrak{l}$ *is nilpotent and of exponent* 2, *or* $\mathfrak{l}$ *contains an idempotent* $e$ *and* $\mathfrak{l} = Te$.

From ($\alpha$) and ($\beta$) it follows that the set of all minimal left ideals of $A$ is closed under right-hand multiplication by elements of $A$. Consequently, in order to prove our theorem it will be sufficient to establish the validity of item (ii). Our theorem is evidently valid when $A$ contains only one minimal non-zero left ideal. So we assume that $A$ contains more than one of these ideals. In order to simplify our phraseology we shall agree that the symbol $\mathfrak{l}$—with or without a subscript—will always denote a minimal non-zero left ideal of $A$.

Let $\mathfrak{l}_1$ be any fixed $\mathfrak{l}$ and let $\mathfrak{l}_2$ be a fixed $\mathfrak{l}$ different from $\mathfrak{l}_1$. We define $\mathfrak{L}_1$ and $\mathfrak{L}_2$ to be $\mathfrak{l}_1$ and $(\mathfrak{l}_1, \mathfrak{l}_2)$ respectively, where $(\mathfrak{l}_1, \mathfrak{l}_2)$ is the ideal-sum of $\mathfrak{l}_1$ and $\mathfrak{l}_2$. Suppose that $\mathfrak{L}_i$ has already been defined for $i < j$. Then we define $\mathfrak{L}_j$ to be the sum $(\mathfrak{L}_{j-1}, \mathfrak{l}_j)$, where $\mathfrak{l}_j$ is any fixed $\mathfrak{l}$ not contained in $\mathfrak{L}_{j-1}$. Obviously each $\mathfrak{L}_i$ is a left ideal of $A$.

($\delta$) *Each* $\mathfrak{L}_i$ *is the direct sum*[8] $\mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_i$.

This statement is obviously true for $i = 1$. Let us assume that it is valid for all $\mathfrak{L}_i$ with $i < j$. By definition, $\mathfrak{L}_j = (\mathfrak{L}_{j-1}, \mathfrak{l}_j)$, where $\mathfrak{l}_j$ is not contained in $\mathfrak{L}_{j-1}$. But $[\mathfrak{L}_{j-1}, \mathfrak{l}_j] = 0$, since this cross-cut is a minimal left ideal contained properly in $\mathfrak{l}_j$. So $\mathfrak{L}_j = \mathfrak{L}_{j-1} + \mathfrak{l}_j$, and from the induction-hypothesis we obtain $\mathfrak{L}_j = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_j$.

Consider the ascending chain

$C_1$: $\mathfrak{L}_1 \subset \mathfrak{L}_2 \subset \cdots$. Let $\mathfrak{S}_1$ denote the element-sum (Vereinigungsmenge) of the terms in $C_1$. Now by definition $\mathfrak{S}_1$ is the set of all elements which occur in at least one $\mathfrak{L}$ (with finite subscript). If $x$ and $y$ are any two elements of $\mathfrak{S}_1$, then there is in $C_1$ an $\mathfrak{L}$ which contains both $x$ and $y$. Since this $\mathfrak{L}$ must contain $x - y$, as well as $zx$ and $zy$, $z$ arbitrary in $A$, it follows that $\mathfrak{S}_1$ is a left ideal of $A$.

From the chain $C_1$ we construct a second chain $C_2$: $\mathfrak{L}_2' \subset \mathfrak{L}_3' \subset \cdots$, where $\mathfrak{L}_i'$ is obtained from $\mathfrak{L}_i$ by deleting the component $\mathfrak{l}_1$—i.e. $\mathfrak{L}_i' = \mathfrak{l}_2 + \mathfrak{l}_3 + \cdots + \mathfrak{l}_i$. Assuming that the chain $C_k$ has already been constructed, we define $C_{k+1}$ to be the ascending chain derived from $C_k$ by deleting from each term in $C_k$ the component $\mathfrak{l}_k$. As in the case of $C_1$ above, we can show that the element-sum for each chain $C_i$ is a left ideal $\mathfrak{S}_i$ of $A$. If $\mathfrak{S}_i \supset 0$, then $\mathfrak{S}_i \supset \mathfrak{S}_{i+1}$; for $\mathfrak{S}$ contains $\mathfrak{l}_i$ while $\mathfrak{S}_{i+1}$ does not (see ($\delta$) above).

Since $A$ is an MLI ring, the descending chain of left ideals $\mathfrak{S}_1 \supset \mathfrak{S}_2 \supset \cdots$ must end with the ideal (0) after a finite number of terms. But this requires that the chain $C_1$ terminate in an $\mathfrak{L}$ with finite subscript—in $\mathfrak{L}_n$, say. That is, $\mathfrak{S}_1 = \mathfrak{L}_n = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n$.

From the definition of the $\mathfrak{L}$'s in $C_1$ we see that $\mathfrak{L}_n$ contains every non-zero minimal left ideal of $A$. Now any subring of $A$ having this property must contain $\mathfrak{L}_n$, since $\mathfrak{L}_n$ is the direct sum of minimal non-zero left ideals. Hence $\mathfrak{L}_n = \mathfrak{M}$, and our proof is completed.

---

[8] Throughout this paper the plus sign will be used only when the sum is direct.

A subring of a ring $T$ is called a *completely-reducible left (right) ideal* if it is the direct sum of a finite number of minimal left (right) ideals of $T$. Thus the ring $\mathfrak{M}$ above is the greatest completely-reducible left ideal of $A$, and we shall usually refer to $\mathfrak{M}$ by this characterization.

In the course of proving Theorem 1.2 we constructed a particular direct decomposition for $\mathfrak{M}$. From the theory of abelian groups with operators we obtain an answer to the "uniqueness-question" regarding the components $\mathfrak{l}_1, \mathfrak{l}_2, \cdots \mathfrak{l}_n$.

2.2: *In any two direct decompositions* (1) $\mathfrak{M} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n$ and (2) $\mathfrak{M} = \mathfrak{l}'_1 + \cdots + \mathfrak{l}'_{n'}$, *where the components are minimal non-zero left ideals, the number of components is the same and the subscripts in* (2) *can be so chosen that* $\mathfrak{l}_i$ *and* $\mathfrak{l}'_i$ *are operator-isomorphic with respect to the elements of* $A$ *as left-hand operators.*[9]

Let us now inquire into the structure of $\mathfrak{M}$. From ($\gamma$) above we know that a minimal non-zero left ideal is either idempotent or nilpotent. For those which are nilpotent we have the following result.

2.3: *The sum* $\mathfrak{N}$ *of all minimal non-zero nilpotent left ideals of* $A$ *is a nilpotent two-sided ideal of exponent* 2.

Proof: Obviously $\mathfrak{N}$ is contained in $\mathfrak{M}$ and is a left ideal of $A$. Now any left ideal contained in a completely-reducible left ideal is itself completely-reducible.[10] So we have $\mathfrak{N} = \mathfrak{n}_1 + \cdots + \mathfrak{n}_k$, where each $\mathfrak{n}_i$ is a minimal non-zero nilpotent ideal. Now $\mathfrak{N}^2 = \sum \mathfrak{n}_i\mathfrak{n}_j = 0$ (see 1.1). Hence $\mathfrak{N}$ is nilpotent and of exponent 2. Moreover, $(\mathfrak{N}_iA)^2 \subseteq \mathfrak{n}_i^2 = 0$. Since $\mathfrak{N}_iA$ is the sum of minimal left ideals (see ($\alpha$) and ($\beta$) above), it follows that $\mathfrak{N}$ is a right, as well as a left, ideal of $A$.

From 1.1 we have $R\mathfrak{N} = \sum R\mathfrak{n}_i = 0$; hence $\mathfrak{N} \subset N_1$. In fact $\mathfrak{N} = [N_1, \mathfrak{M}]$, where $N_1$ is the right annihilator of $R$ in $R$. We state this result in the form of a theorem.

2.4: *The sum of all minimal non-zero nilpotent left ideals of* $A$ *is the cross-cut of the right annihilator of* $R$ *in* $R$ *with the greatest completely-reducible left ideal of* $A$.

It is easy to see that $\mathfrak{N} = 0$ implies $R = 0$, and conversely. We wish to show that $\mathfrak{N} = 0$ also implies $\mathfrak{M} = A$. Suppose that $\mathfrak{N} = 0$ and $\mathfrak{M} \subset A$. Then the set of all left ideals not in $\mathfrak{M}$ contains at least one minimal left ideal $\mathfrak{b}$. Now $\mathfrak{b}$ must contain at least one minimal non-zero left ideal $\mathfrak{l}$ of $A$. Since $\mathfrak{N} = 0$ we have $\mathfrak{l}^2 = \mathfrak{l} = Ae$, where $e^2 = e$. Since $\mathfrak{b}$ is not contained in $\mathfrak{M}$, there is at least one element $b$ in $\mathfrak{b}$ which does not occur in $\mathfrak{M}$. For this element we evidently have $b - be \neq 0$. Let us denote $b - be$ and $(b - be, A(b - be))$ by $\bar{b}$ and $\bar{\mathfrak{b}}$ respectively. Now the left ideal $\bar{\mathfrak{b}}$ is contained properly in $\mathfrak{b}$, since $\mathfrak{b} \supset \mathfrak{l}$ while $[\bar{\mathfrak{b}}, \mathfrak{l}] = 0$. Furthermore, $\bar{\mathfrak{b}}$ is not contained in $\mathfrak{M}$, since the element $\bar{b}$ is not in $\mathfrak{M}$. From the definition of $\mathfrak{b}$, however, we know that $\bar{\mathfrak{b}}$ cannot be contained properly in $\mathfrak{b}$. Hence the assumption $A \supset \mathfrak{M}$ must be abandoned.

[9] This result is a direct consequence of a theorem of Krull (Kr, p. 171).

[10] Kr., p. 171.

So we have $A = \mathfrak{M}$, and from 2.1 we see that $A$ is the direct sum of a finite number of minimal left ideals. So if $\mathfrak{N} = 0$ we have the well-known theorem: *a semi-simple ring is the direct sum of a finite number of minimal left ideals.*

**3.** Throughout this section we shall assume that $A$ is an MLI ring with radical $R \supset 0$. If $R \supset 0$, then $\mathfrak{N} \supset 0$. Evidently we have the two possibilities $\mathfrak{N} = \mathfrak{M}$ and $\mathfrak{N} \subset \mathfrak{M}$. In this section, however, we shall deal only with the case $\mathfrak{N} \subset \mathfrak{M}$.

By the expression *direct complement of* $\mathfrak{N}$ *in* $\mathfrak{M}$ we mean any left ideal $\mathfrak{L}$ of $A$ in $\mathfrak{M}$, such that $\mathfrak{M} = \mathfrak{L} + \mathfrak{N}$. Since $\mathfrak{M}$ is a completely-reducible left ideal, it contains at least one direct complement[11] $\mathfrak{L}$ of $\mathfrak{N}$.

Obviously $\mathfrak{L}$ can contain no non-zero nilpotent left ideals of $A$; hence $\mathfrak{L}$ is the direct sum of minimal idempotent left ideals—$\mathfrak{L} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_s$—and we can assume that the generating idempotents $e_1, \cdots e_s$, of $\mathfrak{l}_1, \cdots \mathfrak{l}_s$ respectively, are orthogonal idempotents[12]—i.e. $e_ie_j = e_je_i = 0$, $i \neq j$; $e_i^2 = e_i$. Since we shall refer to these results later, we collect them in the form of a theorem.

3.1: *One can always find at least one direct complement of* $\mathfrak{N}$ *in* $\mathfrak{M}$; *any direct complement of* $\mathfrak{N}$ *in* $\mathfrak{M}$ *is the direct sum of minimal idempotent left ideals of* $A$ *whose generating idempotents are orthogonal.*

The following theorem exhibits several interesting properties of a direct complement of $\mathfrak{N}$ in $\mathfrak{M}$.

3.2: *Let* $\mathfrak{L}$ *be any fixed direct complement of* $\mathfrak{N}$ *in* $\mathfrak{M}$. *Then* $\mathfrak{L}$ *has the following properties*: (a) $\mathfrak{L}$ *is a semi-simple ring*; (b) *a left ideal of* $\mathfrak{L}$ *is a left ideal of* $A$; (c) *if* $e$ *is the principal unit of* $\mathfrak{L}$, *then* $\mathfrak{L} = eAe$, $\mathfrak{r}_e \subset \mathfrak{l}_e$, $A = \mathfrak{L} + e\mathfrak{l}_e + \mathfrak{r}_e$, *where* $\mathfrak{l}_e$ *and* $\mathfrak{r}_e$ *are respectively the left and right annihilators of* $e$ *in* $A$; (d) $\mathfrak{L}$ *is a right ideal of* $A$ *modulo* $N_1$; (e) $\mathfrak{N}\mathfrak{L} = 0$ *and* $\mathfrak{L}\mathfrak{N} = e\mathfrak{N}$.

Proof: From 3.1 we know that $\mathfrak{L}$ is the direct sum of minimal idempotent left ideals of $A$. Suppose that $\mathfrak{L} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_s = Ae_1 + \cdots + Ae_s$, where the idempotents $e_i$ are orthogonal. Let $e$ denote the sum $e_1 + \cdots + e_s$, and consider the decomposition

(1) $A = eAe + e\mathfrak{l}_e + \mathfrak{r}_e e + \mathfrak{c}$, where $\mathfrak{c} = [\mathfrak{l}_e, \mathfrak{r}_e]$.

Since $\mathfrak{L} = Ae = eAe + _{\mathfrak{L}}\mathfrak{r}_e e$, if we can show that $\mathfrak{r}_e e = 0$ we shall have established 3.2 (c) above.

So we assume $\mathfrak{r}_e e \supset 0$, and for convenience we shall drop the subscript $e$ from both $\mathfrak{l}_e$ and $\mathfrak{r}_e$. *Now* $\mathfrak{re}$ *is a two-sided ideal of* $\mathfrak{L}$. For $\mathfrak{L} \cdot \mathfrak{re} = Ae\mathfrak{re} = 0$, while $\mathfrak{re} \cdot \mathfrak{L} = \mathfrak{re}Ae = \mathfrak{re}(eAe + \mathfrak{re}) = \mathfrak{re}$. Obviously $(\mathfrak{re})^2 = \mathfrak{re}\mathfrak{re} = 0$.

We now construct $\mathfrak{r}^* = (\mathfrak{re}, \mathfrak{re}A)$, which is clearly a right ideal of $A$. But $\mathfrak{re}A = \mathfrak{re}(eAe + e\mathfrak{l} + \mathfrak{re} + \mathfrak{c}) = (\mathfrak{re}, \mathfrak{rel}) = \mathfrak{r}^*$.

Now $\mathfrak{rel} \subseteq \mathfrak{l}$, since $\mathfrak{l}$ is a left ideal. But $\mathfrak{rel}$ is also contained in $\mathfrak{M}$, since $\mathfrak{re} \subseteq \mathfrak{L} \subset \mathfrak{M}$. Hence $\mathfrak{rel} \subseteq [\mathfrak{M}, \mathfrak{l}]$. But $[\mathfrak{M}, \mathfrak{l}] = [\mathfrak{N}, \mathfrak{l}]$; for $[\mathfrak{M}, \mathfrak{l}] = [(\mathfrak{l} + \mathfrak{N}), \mathfrak{l}]$,

[11] Kr, p. 171.

[12] v.d.W.II, p. 159.

and this cross-cut must be annihilated on the right by $e$. Since $[\mathfrak{N}, \mathfrak{l}]$ is a nilpotent left ideal of $A$, and since $\mathfrak{r}e\mathfrak{l} \subseteq [\mathfrak{N}, \mathfrak{l}]$, it follows that $\mathfrak{r}e\mathfrak{l}$ is itself nilpotent. Since $\mathfrak{N}^2 = 0$, we must have $(\mathfrak{r}e\mathfrak{l})^2 = 0$.

By an easy computation we can show that $(\mathfrak{r}^*)^4 = 0$. Thus $\mathfrak{r}^*$ is a nilpotent right ideal of $A$. Moreover, we know that the left ideal $(\mathfrak{r}^*, A\mathfrak{r}^*)$ is nilpotent; hence the cross-cut $\mathfrak{d}$ of $\mathfrak{L}$ with this ideal is a nilpotent left ideal of $A$. Now $\mathfrak{d} \supset 0$; for $\mathfrak{d} \supseteqq \mathfrak{r}e$, and $\mathfrak{r}e \supset 0$. But $\mathfrak{d} \subseteq \mathfrak{L}$ contradicts the fact that $\mathfrak{L}$ contains no non-zero nilpotent left ideal of $A$. Hence the assumption $\mathfrak{r}e \supset 0$ must be abandoned.

From $\mathfrak{r}e = 0$ we obtain immediately the equations $\mathfrak{L} = eAe$, $\mathfrak{c} = \mathfrak{r}$. For the components in the decomposition, $A = eAe + e\mathfrak{l} + \mathfrak{r}$ we have the following multiplication table.

| | $eAe$ | $e\mathfrak{l}$ | $\mathfrak{r}$ |
|---|---|---|---|
| $eAe$ | $eAe$ | $e\mathfrak{l}$ | 0 |
| $e\mathfrak{l}$ | 0 | 0 | $\subseteq e\mathfrak{l}$ |
| $\mathfrak{r}$ | 0 | 0 | $\subseteq \mathfrak{r}$ |

From this table it is evident that a left ideal of $\mathfrak{L}$ is also a left ideal of $A$ (3.2 (b)); hence $\mathfrak{L}$ is an MLI ring. And since $\mathfrak{L}$ is a ring without radical—for a radical of $\mathfrak{L}$ would be a nilpotent left ideal of $A$—we see that $\mathfrak{L}$ is semi-simple (3.2 (a)). From the table we also see that $\mathfrak{L}$ is a right ideal modulo $e\mathfrak{l}$—and also modulo $N_1$, since $e\mathfrak{l} \subseteq N_1$ (3.2 (d)). Finally, from the fact that $\mathfrak{N}$ is contained in $e\mathfrak{l} + \mathfrak{r}$ we obtain $\mathfrak{N}\mathfrak{L} = 0$ and $\mathfrak{L}\mathfrak{N} = e\mathfrak{N}$ (3.2 (e)).

One can easily show by an example that $\mathfrak{N}$ does not always have a unique direct complement in $\mathfrak{M}$. The following theorem affords a means of constructing all direct complements of $\mathfrak{N}$ from a fixed complement $\mathfrak{L}$.

3.3: (a) *If $\mathfrak{L}$ is any fixed direct complement of $\mathfrak{N}$ in $\mathfrak{M}$, then $\mathfrak{L}' = \mathfrak{L}(e + d)$ is a direct complement of $\mathfrak{N}$ in $\mathfrak{M}$, where $e$ is the principal unit of $\mathfrak{L}$ and $d$ is any element of $\mathfrak{M}\mathfrak{N}$; if $d_1 \neq d_2$, then $\mathfrak{L}(e + d_1) \neq \mathfrak{L}(e + d_2)$.*

(b) *If $\mathfrak{L}$ and $\mathfrak{L}'$ are any two direct complements of $\mathfrak{N}$, with principal units $e$ and $e'$ respectively, then $e' = e + d$, where $d \in \mathfrak{M}\mathfrak{N}$; $\mathfrak{L}' = \mathfrak{L}e'$; $\mathfrak{L}$ and $\mathfrak{L}'$ are operator-isomorphic under the correspondence defined by $xe \to xe'$, $x$ variable in $A$.*

(c) *The number of distinct complements of $\mathfrak{N}$ in $\mathfrak{M}$ is equal to the number of elements in $\mathfrak{M}\mathfrak{N}$.*

Obviously (c) is a direct consequence of (a) and (b). We shall give merely an outline of the proofs for (a) and (b), since the details are easily supplied.

Since $\mathfrak{M} = \mathfrak{L} + \mathfrak{N}$ and $\mathfrak{N}^2 = 0$, we have $\mathfrak{M}\mathfrak{N} = \mathfrak{L}\mathfrak{N} = e\mathfrak{L}e\mathfrak{N} = e\mathfrak{N}$. Let $d$ be any element of $e\mathfrak{N}$ and denote $e + d$ by $e'$ and $\mathfrak{L}e'$ by $\mathfrak{L}'$. It is easy to show that $[\mathfrak{L}', \mathfrak{N}] = 0$ and that every element of $\mathfrak{M}$ can be represented as the sum of an element of $\mathfrak{L}'$ and an element of $\mathfrak{N}$. Hence $\mathfrak{L}'$ is a direct complement of $\mathfrak{N}$ in $\mathfrak{M}$.

To prove the second part of 3.3 (a) we first observe that $e' = e + d$ is idempotent; this follows from the equations $e^2 = e$, $ed = d$, $d^2 = 0$, $de = 0$ (see

3.2 (e)). Hence $e'$ is a right-hand identity for $\mathfrak{L}e'$. Suppose, now, that $d_1$ and $d_2$ are two distinct elements of $e\mathfrak{N}$. To show that $\mathfrak{L}(e + d_1) \neq \mathfrak{L}(e + d_2)$ it is sufficient to show that $e + d_1$ is not contained in $\mathfrak{L}(e + d_2)$. If it were, $e + d_2$ would have to be a right-hand identity for $e_1 + d_1$. But by computation we find that $(e_1 + d_1)(e_1 + d_2) = e_1 + d_2$. Hence different choices for $d$ lead to different complements of $\mathfrak{N}$ in $\mathfrak{M}$.

Proof of 3.3 (b): Let $\mathfrak{L}$ and $\mathfrak{L}'$ be any two direct complements of $\mathfrak{N}$ in $\mathfrak{M}$ and let $e$ denote the principal unit of $\mathfrak{L}$. Let $f$ and $g$ denote the components of $e$ in $\mathfrak{L}'$ and $\mathfrak{N}$ respectively. From $e^2 = e$ and $gf = 0$ we can derive $f^2 = f$ and $fg = g$. By squaring $f = e - g$ we find that $eg = g$. That is, $f$ is of the form $f = e + d$, $d \in e\mathfrak{N}$. From 3.3 (a) it follows that $\mathfrak{L}f$ is a direct complement of $\mathfrak{N}$ in $\mathfrak{M}$.

From the fact that $e$ is the principal unit of $\mathfrak{L}$, together with the equation $\mathfrak{N}\mathfrak{L} = 0$, one can easily show that $f$ is the principal unit of $\mathfrak{L}f$. Now from $f \in \mathfrak{L}'$ we obtain $\mathfrak{L}f \subseteq \mathfrak{L}'$. But $\mathfrak{L}f$ and $\mathfrak{L}'$ are isomorphic, since they are both direct complements of $\mathfrak{N}$ in $\mathfrak{M}$. Hence $\mathfrak{L}' = \mathfrak{L}f = \mathfrak{L}(e - g)$, where $f(= e')$ is the principal unit of $\mathfrak{L}'$.

Now the correspondence $y \to ye'$, for $y$ variable in $\mathfrak{L}$, defines an operator-homomorphism of $\mathfrak{L}$ with $\mathfrak{L}'$ (see 2 ($\alpha$)). Since $ye' = y + \bar{y}$, $\bar{y} \in N$, we see that $ye' = 0$ requires $y = 0$. Hence the homomorphism above is an isomorphism. Since $\mathfrak{L}$ and $\mathfrak{L}'$ are left ideals, this isomorphism is evidently the same as the isomorphism defined by $xe \to xe'$, $x$ variable in $A$. This completes the proof of 3 (b).

Up to this point we have been concerned mainly with the component $\mathfrak{L}$ in the decomposition $A = \mathfrak{L} + e\mathfrak{l}_e + \mathfrak{r}_e$ (see 3.2 (c)). Let us now examine the component $\mathfrak{l}_e(= e\mathfrak{l}_e + \mathfrak{r}_e)$. From the multiplication table above we see that $\mathfrak{l}_e$ is a two-sided ideal of $A$. By definition, $\mathfrak{l}_e$ is the left annihilator of $e$; since $\mathfrak{L} = e\mathfrak{L}$, it is easy to show that $\mathfrak{l}_e$ is also the left annihilator of $\mathfrak{L}$.

From 3.3 (b) we know that any two direct complements $\mathfrak{L}$ and $\mathfrak{L}'$ of $\mathfrak{N}$ are operator-isomorphic under the correspondence $xe \to xe'$. Hence $\mathfrak{l}_e = \mathfrak{l}_{e'}$, and since $\mathfrak{l}_e(\mathfrak{l}_{e'})$ is the left annihilator of $\mathfrak{L}(\mathfrak{L}')$, it follows that any two direct complements of $\mathfrak{N}$ have the same left annihilator.[13] We have, then, the following theorem.

3.4: *Any two direct complements of $\mathfrak{N}$ in $\mathfrak{M}$ have the same left annihilator $\mathfrak{l}$, and $\mathfrak{l}$ is a two-sided ideal of $A$.*

This ends our investigation of the structure of $A$ by means of its greatest completely-reducible left ideal $\mathfrak{M}$. We conclude this section by pointing out a direction which further investigations might take. One may construct the quotient-ring $A' = A/(\mathfrak{M}, N_1)$, determine the greatest completely-reducible left ideal[14] $\mathfrak{M}_2'$ of $A$ contained in $A'$; discuss the homomorphic image $\mathfrak{M}_2$ of $\mathfrak{M}_2'$ in $A$. One readily sees that $A/(\mathfrak{M}, N_1)$ is isomorphic with $\mathfrak{l}_e/N_1$; hence $\mathfrak{M}_2$ is

[13] One can also prove that $e\mathfrak{l}_e = e'\mathfrak{l}_{e'}$. It is interesting to note, however, that $\mathfrak{r}_e$ need not equal $\mathfrak{r}_{e'}$.

[14] See definition of the term "ideal of $A$" given at the end of the Introduction.

contained entirely in $\mathfrak{l}_e$. In constructing $\mathfrak{M}_2'$ and $\mathfrak{M}_2$, however, we cannot disregard $\mathfrak{L}$; for unless $\mathfrak{L}$ is a two-sided ideal of $A$ we cannot be sure that $\mathfrak{l}_e$ is an MLI ring. If $\mathfrak{N}_2'$ is the sum of all nilpotent left ideals of $A$ in $\mathfrak{M}_2'$, $\mathfrak{L}_2'$ a direct complement of $\mathfrak{N}_2'$ in $\mathfrak{M}_2'$ (in case $\mathfrak{N}_2' \subset \mathfrak{M}_2'$), $\mathfrak{L}_2$ the homomorphic image of $\mathfrak{L}_2'$ in $A$, then we can show that $\mathfrak{L}_2$ contains a right-hand identity $e_2$, which is a left-hand identity of $\mathfrak{L}_2$ modulo $N_1$. For $A$ we should then have the direct decomposition $A = \mathfrak{L}_1 + \mathfrak{L}_2 + \mathfrak{l}_{e_2} = Ae + Ae_2 + \mathfrak{l}_{e_2}$, $\mathfrak{l}_{e_2}$ being the left annihilator of $e_2$ in $\mathfrak{l}_e$. Since $R = N_{\rho-1}$ (see 1.4), a continuation of this construction will lead to the known result[15] that a semi-primary ring is the direct sum of idempotent left ideals, each containing a right-hand identity, plus a left ideal from the radical. From the construction outlined above, however, we obtain more than an "existence theorem": e.g. $\mathfrak{L}$ is a semi-simple ring and a right ideal modulo $N_1$ (see 3.2); $\mathfrak{L}_2$ is a semi-simple ring modulo $N_1$ and a right ideal of $A$ modulo $N_2$ etc.

**4.** In the preceding sections we have been concerned with properties of MLI rings of the greatest generality. From this point on we shall deal mainly with two special types of MLI rings; the nilpotent and the idempotent MLI rings. First, however, we shall establish several preparatory theorems.

In §1 we pointed out that the radical $R$ of an MLI ring $A$ is nilpotent and that the quotient-ring $A' = A/R$ is semi-simple. So if $A = R$ then $A$ is necessarily nilpotent; while if $A \supset R$, then $A'$ contains an idempotent $e'$, and by a construction due to Köthe[16] we can find in $A$ an idempotent $e$ which corresponds to $e'$ in the homomorphism $A \sim A'$. But an MLI ring which contains an idempotent must contain[17] a principal[18] idempotent. The results in this paragraph may be conveniently expressed as the following theorem.

4.1: *An* MLI *ring is either nilpotent or it contains a principal idempotent.*

We shall need the following result, which is proved[19] in Deuring's *Algebren*.

(a) *If $e$ is any idempotent of the* MLI *ring $A$, then in the decomposition $A = eAe + e\mathfrak{L} + \mathfrak{R}e + [\mathfrak{L}, \mathfrak{R}]$, both $eAe$ and $[\mathfrak{L}, \mathfrak{R}]$ are* MLI *rings.*

By a slight modification of one of Dickson's[20] proofs we obtain the following theorem.

4.2: *If $e$ is a principal idempotent of the* MLI *ring $A$, then in the decompositions $A = Ae + \mathfrak{L}$ and $A = eA + \mathfrak{R}$, both $\mathfrak{L}$ and $\mathfrak{R}$ are contained in the radical $R$ of $A$.*

Suppose, now, that the MLI ring $A$ contains two distinct principal idempotents $e_1$ and $e_2$. From Theorem 4.2 it is easy to see that the homomorphic

---

[15] D, p. 16.
[16] D, p. 16.
[17] D, p. 14.
[18] If a ring $T$ contains an idempotent $e$ but no second idempotent $u$ such that $eu = ue = 0$, then $e$ is called a principal idempotent. D 1, p. 49.
[19] D, p. 14.
[20] D 2, p. 100.

images $e_1'$ and $e_2'$ in $A'$ of $e_1$ and $e_2$ respectively are principal units of the semi-simple ring $A'$. Since a ring can contain only one principal unit, we must have $e_1' = e_2'$, and from this it follows directly that $e_1 = e_2 + r$, where $r$ is an element in the radical $R$ of $A$.

Consider now the two decompositions

$$(1) \qquad A = e_1Ae_1 + e_1\mathfrak{L}_1 + \mathfrak{R}_1e_1 + \mathfrak{C}_1, \qquad \mathfrak{C}_1 = [\mathfrak{L}_1, \mathfrak{R}_1] \text{ and}$$

$$(2) \qquad A = e_2Ae_2 + e_2\mathfrak{L}_2 + \mathfrak{R}_2e_2 + \mathfrak{C}_2, \qquad \mathfrak{C}_2 = [\mathfrak{L}_2, \mathfrak{R}_2].$$

From the equation $e_1\mathfrak{C}_1e_1 = 0$, together with the fact that $r$ and $\mathfrak{C}_1$ are in $R$ we find that $e_2\mathfrak{C}_1e_2 = r\mathfrak{C}_1r \subseteq R^3$. Now if the radical $R$ is of exponent $\rho \leqq 3$, then $e_2\mathfrak{C}_1e_2 = 0$; and from this we obtain $\mathfrak{C}_1 \subseteq \mathfrak{C}_2$. In a similar manner we can show that $\rho \leqq 3$ implies $\mathfrak{C}_i \supseteq \mathfrak{C}_2$. So we obtain the following theorem.

4.3: *If $e_1$ and $e_2$ are any two principal idempotents of an* MLI *ring $A$, then in the decompositions* (1) *and* (2) *above we must have* $[\mathfrak{L}_1, \mathfrak{R}_1] = [\mathfrak{L}_2, \mathfrak{R}_2]$ *whenever the exponent of the radical of $A$ does not exceed* 3.

Our proof obviously depends upon the assumption $R^3 = 0$. Whether the theorem holds for $\rho > 3$ is still an open question.

We conclude this section by proving a very useful lemma.

4.4: *If $A$ is an* MLI *ring* (MRI *ring*), *and if* $A = (\mathbf{a},\mathbf{b})$, *where* $\mathbf{a}$ *is a subring of $A$ and* $\mathbf{b}$ *is a subring of the radical $R$ of $A$, then* $\mathbf{a}$ *is an* MLI *ring* (MRI *ring*).

We shall give the proof only for the case where $A$ is an MLI ring. Suppose that $\mathbf{a}$ contains an infinite descending chain[21] of left ideals of $\mathbf{a}$:

$$(3) \qquad \mathfrak{l}_1 \supset \mathfrak{l}_2 \supset \cdots,$$

where $\mathfrak{l}_i$ is a left ideal of $\mathbf{a}$ (but not necessarily of $A$). Let us denote $(\mathfrak{l}_i, \mathbf{b}\mathfrak{l}_i)$ by $\mathfrak{l}_i^*$. Now each $\mathfrak{l}_i^*$ is a left ideal of $A$, and since $A$ is an MLI ring there exists a finite subscript $k$ such that $\mathfrak{l}_k^* = \mathfrak{l}_{k+1}^* = \cdots$. To simplify the notation, let us think of (3) as beginning with the first $\mathfrak{l}_i$ for which $\mathfrak{l}_i^* = \mathfrak{l}_{i+1}^*$. That is, we assume $\mathfrak{l}_1^* = \mathfrak{l}_2^* = \cdots$.

Since each $\mathbf{b}\mathfrak{l}_i$ is contained in $R$, we have the equalities

$$(4) \qquad (\mathfrak{l}_1^*, R) = (\mathfrak{l}_2^*, R) = \cdots = (\mathfrak{l}_1, R) = (\mathfrak{l}_2, R) = \cdots.$$

Since the submoduli of any modulus (additive abelian group) satisfy the Dedekind (modular) axiom, we obtain the equations

$$(5) \qquad \mathfrak{l}_1 = (\mathfrak{l}_2, [\mathfrak{l}_1, R]) = (\mathfrak{l}_3, [\mathfrak{l}_2, R], [\mathfrak{l}_1, R]) = \cdots.$$

Now from (3) it is evident that the cross-cuts $[\mathfrak{l}_1, R]$, $[\mathfrak{l}_2, R]$ etc. must form an infinite descending chain of left ideals of $\mathbf{a}$ and in $R$. So in proving 4.4 we may assume that each $\mathfrak{l}_i$ in (3) is contained in the radical $R$ of $A$.

(i) Suppose that $\mathfrak{l}_1$ is in the right annihilator $N_1$ of $R$. Then $\mathfrak{l}_1^* = \mathfrak{l}_2^* = \cdots$

[21] By the phrase *infinite descending chain* we mean a chain of infinite length in which each term is contained properly in the preceding. Later we shall attach a corresponding meaning to the phrase *infinite ascending chain.*

would imply $\mathfrak{l}_1 = \mathfrak{l}_2 = \cdots$, since $\mathbf{b}\mathfrak{l}_i \subseteq RN_1 = 0$. It follows, then, that the first term of (3) cannot be contained in $N_1$.

(ii) As a basis for induction, let us assume that no infinite descending chain of left ideals of $\mathbf{a}$ can be contained in $N_i$, $1 \leqq i < s$. Since $R = N_{\rho-1}$, where $\rho$ is the exponent of $R$ (see proof of 1.4), our theorem will be established if we can show that the first term of (1) cannot be contained in $N_s$.

Suppose that $\mathfrak{l}_1$ is in $N_s$ and not in $N_{s-1}$. From $\mathfrak{l}_1^* = \mathfrak{l}_2^* = \cdots$ and $\mathbf{b}\mathfrak{l}_i \subseteq RN_s \subseteq N_{s-1}$ (see proof of 1.4), we obtain $\mathfrak{l}_1 \equiv \mathfrak{l}_2 \bmod N_{s-1}$. Exactly as above we can show that the conditions $\mathfrak{l}_1 \supset \mathfrak{l}_2 \cdots$ and $\mathfrak{l}_1 \equiv \mathfrak{l}_2 \equiv \cdots \bmod N_{s-1}$ are consistent only if $[\mathfrak{l}_1, N_{s-1}]$, $[\mathfrak{l}_2, N_{s-1}]$, $\cdots$ form an infinite descending chain. But each of these cross-cuts is a left ideal of $\mathbf{a}$ and in $N_{s-1}$. From our induction-hypothesis, however, we know that $N_{s-1}$ contains no infinite descending chain of left ideals of $\mathbf{a}$. This completes the proof of 4.4.

**5.** In this section we shall deal exclusively with nilrings. One can easily show by examples that in the case of a non-nilpotent ring the minimal (maximal) condition for left ideals does not necessarily imply the minimal (maximal) condition for right ideals. For nilrings, however, we have the following interesting results.

5.1: *If $B$ is a nilring, then the minimal condition for left ideals implies the minimal condition for right ideals, and conversely.*

5.2: *If $B$ is a nilring, then the maximal condition for left ideals implies the maximal condition for right ideals, and conversely.*

Proof of 5.1: If $B$ is an MLI nilring it is necessarily nilpotent (see 1.4), and we must have $B = R$. Let $\rho$ denote the exponent of $B$. Suppose that $B$ contains the infinite descending chain

(1) $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$, in which each $\mathfrak{a}_i$ is a right ideal of $B$.

(i) We consider first the possibility that $\mathfrak{a}_1$ is in $N_1$, the right annihilator of $B$. Then each term in (1) is a left ideal of $B$, from the fact that $B\mathfrak{a}_i \subseteq BN_1 = 0$. This proves that $\mathfrak{a}_1$ cannot be contained in $N_1$, since $B$ contains no infinite descending chain of left ideals.

(ii) As a basis for induction, let us assume that for $1 \leqq i < s$ there is no infinite descending chain of right ideals contained in $N_i$. Suppose that $\mathfrak{a}_1$ is contained in $N_s$ but not in $N_{s-1}$. We denote $(\mathfrak{a}_i, N_{s-1})$ by $\mathfrak{a}_i^*$ and observe that $\mathfrak{a}_i^*$ is a left ideal of $B$; this follows from the fact that $B\mathfrak{a}_i \subseteq BN_s \subseteq N_{s-1}$. With no loss of generality we can assume $\mathfrak{a}_1^* = \mathfrak{a}_2^* = \cdots$—i.e. we can delete from (1) those terms, finite in number, for which $\mathfrak{a}_i^* \supset \mathfrak{a}_{i+1}^*$. As in the proof of 4.4, we can show that the conditions $\mathfrak{a}_1^* = \mathfrak{a}_2^* = \cdots$ and $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ are consistent only if the cross-cuts $[\mathfrak{a}_1, N_{s-1}]$, $[\mathfrak{a}_2, N_{s-1}]$ etc. form an infinite descending chain. But each of these cross-cuts is a right ideal of $B$ and in $N_{s-1}$. Thus we reach a conclusion which contradicts our induction-hypothesis.

To show that every MRI nilring is also an MLI ring we need only to interchange the words "left" and "right" in the argument above.

PROOF OF 5.2: Let $B$ denote a nilring with maximal condition for left ideals. Suppose that $B$ contains an infinite ascending chain of right ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots . \tag{2}$$

We denote $(\mathfrak{a}_i, B\mathfrak{a}_i)$ by $\mathfrak{a}_i^*$ and observe that $\mathfrak{a}_i^*$ is a left ideal of $B$. Since we must ultimately have $\mathfrak{a}_k^* = \mathfrak{a}_{k+1}^* = \cdots$, we may assume that the chain (2) begins with the first term for which $\mathfrak{a}_i^* = \mathfrak{a}_{i+1}^* = \cdots$—that is, we assume $\mathfrak{a}_1^* = \mathfrak{a}_2^* = \cdots$.

Since $B\mathfrak{a}_i \equiv 0 \bmod B^2$, we see that $\mathfrak{a}_1^* = \mathfrak{a}_2^* = \cdots$ implies $(\mathfrak{a}_1, B^2) = (\mathfrak{a}_2, B^2) = \cdots$. From the equalities $\mathfrak{a}_i = (\mathfrak{a}_{i-1}, [\mathfrak{a}_i, B^2])$ it is easy to see that the existence of (2) requires that the cross-cuts $[\mathfrak{a}_1, B^2]$, $[\mathfrak{a}_2, B^2]$ etc. constitute an infinite ascending chain, each term of which is a right ideal of $B$ and in $B^2$. Let $\rho$ denote the exponent[22] of $B$. Obviously $B^\rho$ can contain no infinite ascending chain of right ideals, and it is equally obvious that one can complete the proof of 5.2 by induction from $B^k$ to $B^{k-1}$. As in the case of 5.1, one can establish the "conversely" merely by interchanging the words "right" and "left."

If $S$ is any subring of the MLI nilring $B$, then $B = (S, B)$. If we apply 4.4 to this special case and make use of 5.1, we obtain the following theorem.

5.3: *Any subring of an* MLI (MRI) *nilring is itself both an* MLI *and an* MRI *ring.*

The following result is of interest in that it has no counterpart in the case of a non-nilpotent MLI ring.

5.4: *If $B$ is an* MLI (MRI) *nilring, then the minimal condition holds for subrings of $B$—i.e. $B$ cannot contain an infinite descending chain of subrings.*

For if $B$ contains an infinite descending chain $S_1 \supset S_2 \supset \cdots$, where each $S_i$ is a subring (but not necessarily an ideal) of $B$, then $S_i^* (= (S_i, BS_i))$ is a left ideal of $B$, and we ultimately have the equality $S_k^* = S_{k+1}^* = \cdots$. If $S_1$ is contained in $N_i$, but not in $N_{i-1}$, we can show that $N_{i-1}$ must contain the infinite descending $[S_k, N_{i-1}] \supset [S_{k+1}, N_{i-1}] \supset \cdots$. Obviously $S_1$ cannot be contained in $N_1$, and it is easy to complete the proof by induction from $N_i$ to $N_{i+1}$.

We shall now investigate the structure of an MLI nilring $B$ regarded as an additive abelian group $G$. Suppose that $G$ contained an element $x$ of infinite order. Let $X$ and $X_{2^n}$ denote the subrings generated by $x$ and $2^n x$ respectively. Then $B$ would contain the infinite descending chain of subrings $X \supset X_2 \supset X_4 \supset \cdots$. But this is impossible, in view of Theorem 5.4. Hence $G$ contains only elements of finite order.[23]

Now the sum of all minimal left ideals of $B$ is a completely-reducible left ideal $\mathfrak{M}$ of finite length (see 2.1). Since a minimal left ideal of $B$ is necessarily a cyclic group of prime order, we know that $\mathfrak{M}$ is the direct sum of a finite

[22] For a proof that $B$ is nilpotent see v. d. W. II, p. 155 or D, p. 12.

[23] Since the maximal condition need not hold for subrings of $B$, the orders of the elements of $G$ are in general unbounded.

number of cyclic groups: $\mathfrak{M} = C_1 + C_2 + \cdots + C_r$, where each $C_i$ is of prime order $p_i$. If the order $n(x)$ of $x$ is divisible by the prime $p$, then $[X, \mathfrak{M}]$ must contain at least one subgroup of order $p$. It follows, then, that the set of all distinct primes which occur as divisors of $n(x)$, as $x$ varies over the elements of $G$, is a finite set, containing—let us say—the primes $p_1, p_2, \cdots p_t$, $t \leqq r$.

Those elements of $G$ whose orders are powers of the fixed prime[24] $p_i$ constitute a subgroup $G_i$. Since each element of $G$ has a uniquely-determined component in $G_i$, we see that $G$ is the direct sum of the $t$ groups $G_j$. From the distributive law it is easy to see that $G_iG_j = G_jG_i = 0$, $i \neq j$, and $G_j^2 \subseteq G_j$. Thus each $G_j$ is a two-sided ideal of $B$, and we obtain the following structure-theorem.

5.5: *For every* MLI (MRI) *nilring $B$ we have the unique direct decomposition $B = G_1 + G_2 + \cdots + G_t$, where ($\alpha$) $G_1, G_2, G_t$ are primary abelian groups belonging to distinct primes; ($\beta$) each $G_j$ is a two-sided ideal of $B$; ($\gamma$) each $G_j$ is both an* MLI *and an* MRI *ring.*[25]

Thus the theory of MLI nilrings is essentially the theory of MLI nilrings in which the (additive) order of every element is a power of a fixed prime.

**6.** In this section we shall examine the components in the direct decompositions of an MLI ring with respect to a principal idempotent.

Let $J$ denote a non-nilpotent MLI ring, and let $e$ be a principal idempotent of $J$ (see 4.1). Associated with $e$ there are the two direct decompositions

(1) $J = Je + \mathfrak{L}$ and

(2) $J = eJ + \mathfrak{R}$, where $\mathfrak{L}(\mathfrak{R})$ is the left (right) ideal of $J$ consisting of those elements of $J$ which are annihilated on the right (left) by $e$.

We know that both $\mathfrak{L}$ and $\mathfrak{R}$ are contained in the radical $R$ of $J$ (see 4.2). So from Lemma 4.4 we obtain the following result.

6.1: *Both $Je$ and $eJ$ are* MLI *rings.*

Now it is easy to show[26] that the left ideal $\mathfrak{L}$ in (1) above need not be an MLI ring. On the other hand, we have the following result concerning the right ideal $\mathfrak{R}$.

6.2: *In the decomposition $J = eJ + \mathfrak{R}$ the right ideal $\mathfrak{R}$ is both an* MLI *and an* MRI *ring.*

PROOF: Suppose that $\mathfrak{R}$ contains an infinite descending chain

(3) $\mathfrak{l}_1 \supset \mathfrak{l}_2 \supset \cdots$ in which each term is a left ideal of $\mathfrak{R}$. Then $(\mathfrak{l}_i, J\mathfrak{l}_i)$, which we denote by $\mathfrak{l}_i^*$, is a left ideal of $J$. Since we ultimately have $\mathfrak{l}_k^* = \mathfrak{l}_{k+1}^* = \cdots$, we can assume, without loss of generality, that $\mathfrak{l}_1^* = \mathfrak{l}_2^* = \cdots$. Now $J\mathfrak{l}_i = (Je + \mathfrak{L})\mathfrak{l}_i = \mathfrak{L}\mathfrak{l}_i$, since $e\mathfrak{l}_i \subseteq e\mathfrak{R} = 0$. Furthermore, $\mathfrak{L}$ and $\mathfrak{l}_i$ are both contained in the radical $R$ of $J$. Suppose that $\mathfrak{l}_i$ is in $N_s$, but not in $N_{s-1}$; then $\mathfrak{L}\mathfrak{l}_i$ is necessarily contained in $N_{s-1}$, and the inequalities $\mathfrak{l}_1 \supset$

[24] Such a group is known as a primary group belonging to the prime $p_i$.

[25] Property ($\gamma$) is evidently a consequence of 5.3.

[26] Consider $J = Fe + Fu$, where $F$ is the rational field, $e^2 = e$, $eu = u$, $u^2 = ue = 0$. Then $Je = Fe$ and $\mathfrak{L} = Fu$. Obviously no chain condition is satisfied by ideals of $Fu$.

$\mathfrak{l}_2 \supset \cdots$, together with the equalities $\mathfrak{l}_1^* = \mathfrak{l}_2^* = \cdots$, require the existence of an infinite descending chain $[\mathfrak{l}_1, N_{s-1}] \supset [\mathfrak{l}_2, N_{s-1}] \supset \cdots$. Such a chain is obviously impossible for $s = 1$. We shall omit the remainder of the proof (by induction over $s$), since the method has been fully illustrated in the proof of 4.4.

A ring $A$ shall be said to be an MMLI ring if both the minimal and the maximal condition hold for left ideals of $A$. From known considerations it follows that a ring $A$ is an MMLI ring if, and only if, it has a composition series of left ideals of $A$.

6.3: *In the direct decomposition* $J = eJ + \mathfrak{N}$ *the ring* $eJ$ *is an* MMLI *ring.*

Since $eJ$ is an MLI ring (see 6.1), this theorem is equivalent to the following:

6.4: *An* MLI *ring is an* MMLI *ring if it contains a left-hand identity element.*

PROOF: Let $A$ be any MLI ring containing the left-hand identity $e$, and let $R$ denote the radical of $A$. Our theorem is known to be true if $R = 0$, since a semi-simple ring has a composition series of left ideals. So we assume $R \supset 0$. In this case the quotient-ring $A/R(= A')$ is semi-simple (see 1.5). From a composition series of left ideals of $A'$, together with a composition series of left ideals of $A$ in $R$, we can construct for $A$ a composition series of left ideals. To prove our theorem it is therefore sufficient to show that $R$ contains a composition series of left ideals of $A$; and to do this we have only to prove that the quotient-ring $N_{s+1}/N_s$ is contained in the greatest completely-reducible left ideal $\mathfrak{M}'_{s+1}$ of $A/N_s$ (see §§1–2).

Let $x$ and $u$ be any non-zero elements of $A$ and of $N_{s+1}/N_s(= N'_{s+1})$ respectively. We know that $RN_{s+1} \equiv 0 \bmod N_s$; hence $xu = (x + R)u = x'u$, where $x'$ is the homomorphic image of $x$ in $A'$. So we can regard $N'_{s+1}$ as an abelian group with the elements of $A'$ (instead of $A$) as left-hand operators. Since $A$ contains the left-hand identity $e$, the left ideal $(u, Au)$ is equal to $Au$. Since $A'$ is the direct sum of minimal left ideals—$A' = \mathfrak{l}'_1 + \mathfrak{l}'_2 + \cdots + \mathfrak{l}'_k$, say—we have $Au = A'u = \mathfrak{l}'_1u + \mathfrak{l}'_2u + \cdots + \mathfrak{l}'_ku$. Hence every element $u$ of $N'_{s+1}$ is contained in the greatest completely-reducible left ideal $\mathfrak{M}'_{s+1}$ of $A/N_s$, and since $\mathfrak{M}'_{s+1}$ is the direct sum of a finite number of minimal left ideals, it follows that $N'_{s+1}$ has a composition series of left ideals of $A$. But $R = N_{\rho-1}$, where $\rho$ is the exponent of $R$. Hence $R$ itself has a composition series of left ideals of $A$, and our proof is ended.

Up to this point we have been concerned mainly with the decomposition $J = eJ + \mathfrak{N}$. Let us now consider the decomposition $J = Je + \mathfrak{L}$. As we noted above, little can be said regarding the left ideal $\mathfrak{L}$, in contrast to Theorem 6.2 concerning $\mathfrak{N}$. For the component $Je$, however, we are able to obtain several interesting results.

First, we decompose $Je$ into the following direct sum:

$$Je = eJe + \mathfrak{N}e. \tag{4}$$

We shall not investigate the structure of $eJe$ beyond pointing out that it is an MMLI ring (see 6.4). For the component $\mathfrak{R}e$, however, we have the results 6.5, 6.6, and 6.7 below.

6.5: *The maximal condition holds for right ideals of $Je$ in $\mathfrak{R}e$.*

6.6: (a) *The component $\mathfrak{R}e$ is a nilpotent two-sided ideal of $Je$ of exponent 2;* (b) *the additive group of $\mathfrak{R}e$ is of finite order.*

PROOF OF 6.5: We know that $\mathfrak{R}e$ is both an MLI and an MRI ring (see 6.2). Since $\mathfrak{R}e$ is a right ideal of $Je$, it is obvious that the minimal condition must hold for right ideals of $Je$ in $\mathfrak{R}e$. Hence the sum of all minimal right ideals of $Je$ in $\mathfrak{R}e$ is a completely-reducible right ideal $\mathfrak{R}_1$ of finite length.

Let $R$ denote the radical of $Je$, and let $M_1$ denote the left annihilator of $R$ in $R$ (see 1.5). Let $u$ be any non-zero element of $[\mathfrak{R}e, M_1]$. For any element $x$ of $Je$ we have $ux = u(x + R) = ux'$, where $x'$ is the homomorphic image of $x$ in the quotient-ring $J' = Je/R$. Now $J'$ is semi-simple, and it is known that any semi-simple ring is the direct sum of minimal right ideals. So we have $J' = \mathfrak{r}_1' + \cdots + \mathfrak{r}_n'$, where each $\mathfrak{r}_i'$ is a minimal right ideal of $J'$.

Since $u = ue$, we have the equations $(u, uJe) = uJ' = u\mathfrak{r}_1' + \cdots + u\mathfrak{r}_n'$. But each $u\mathfrak{r}_i'$ is either 0 or a minimal right ideal of $Je$ in $\mathfrak{R}e$. Hence $u$ is contained in $\mathfrak{R}_1$, and since $u$ represents any non-zero element of $[\mathfrak{R}e, M_1]$, it follows that $[\mathfrak{R}e, M_1]$ is contained in $\mathfrak{R}_1$. From this we deduce the existence of a composition series of right ideals of $Je$ in $[\mathfrak{R}e, M_1]$.

Now the chain $[\mathfrak{R}e, M_1] \subset [\mathfrak{R}e, M_2] \subset \cdots$ terminates in $\mathfrak{R}e$, since $M_{p-1} = R$ (see 1.5). One can now show by induction that $\mathfrak{R}e$ contains a composition series of right ideals of $Je$; we shall omit the proof, since the details are almost parallel to those in the proof of 6.3. From the existence of this composition series now follows the maximal condition for right ideals of $Je$ in $\mathfrak{R}e$.

PROOF OF 6.6: The theorem is trivial for $\mathfrak{R}e = 0$, so we assume $\mathfrak{R}e \supset 0$. The proof of item (a) is obvious. Now from 6.2 and 5.3 we know that $\mathfrak{R}e$ is an MLI ring, and from 5.5 we know that for $\mathfrak{R}e$ we have a direct decomposition $\mathfrak{R}e = G_1 + G_2 + \cdots + G_t$, where $G_1, \cdots, G_t$ are primary abelian groups belonging to the distinct primes $p_1, \cdots, p_t$. Let $P$, belonging to the prime $p$ denote a fixed one of the components $G_i$. To prove property (b) it is clearly sufficient to show that $P$ is of finite order.

We know that $P$ is not only a right ideal of $\mathfrak{R}e$, but a right ideal of $Je$ as well, since the order of the product $xy$, $x \in P$, $y \in Je$, must be a power of $p$. Let $H_j$ be the set of all elements $x$ in $P$ for which $p^j x = 0$. It is clear that $H_j$ is a subgroup of $P$; furthermore, $H_j$ is a right ideal of $Je$, since the order of $xy$, $x \in P$, $y \in Je$, cannot exceed $p^j$. So from 6.5 we see that in the ascending chain $H_1 \subseteq H_2 \subseteq \cdots$ we must eventually have the equality sign; and if $k$ is the smallest subscript for which $H_k = H_{k+1}$, then $P = H_k$.

We have proved that $p^k$ is an upper bound for the orders of the elements of $P$. To complete our proof we have only to show that each $H_j$ is of finite

order. Since each $H_{i+1}/H_i(=H'_{i+1})$ is the sum of all minimal left ideals of $P/H_i$, it follows from 2.1 that $H'_{i+1}$ is the direct sum of a finite number of minimal left ideals. Since a minimal left ideal of $P$ is a subgroup of order $p$, it follows that the order of $H'_{i+1}$ is finite. This completes the proof of 6.6.

Since $eJe$ is an MMLI ring and since $\mathfrak{N}e$ contains only a finite number of elements, it follows that $Je$ is an MMLI ring. Combining this result with 6.3 we obtain the following theorem.

6.7: *An* MLI *ring is an* MMLI *ring if it contains either a left-hand identity or a right-hand identity.*

We have investigated rather fully the structure of $Je$ in the decomposition $J = Je + \mathfrak{L}$. Such a detailed treatment of the component $eJ$ in $J = eJ + \mathfrak{N}$ is hardly possible for the reason that little can be said about the component $e\mathfrak{L}$ in $eJ = eJe + e\mathfrak{L}$. From results already obtained we know that $e\mathfrak{L}$, which is a nilpotent two-sided ideal of $eJ$ and of exponent 2, has a composition series of left ideals of $eJ$. But regarding ideals of $e\mathfrak{L}$ itself we can in general obtain no information. From the example in Note 26 we see that neither maximal nor minimal condition need hold for left (or right) ideals of $e\mathfrak{L}$.

We shall conclude this section by proving a theorem relating to $[\mathfrak{L}, \mathfrak{N}]$ for the case where $J$ is idempotent. This cross-cut, which we shall denote by $\mathfrak{C}$, occurs in the decomposition

$$J = eJe + e\mathfrak{L} + \mathfrak{N}e + \mathfrak{C}. \tag{5}$$

Since $J$ is idempotent, $J = J^2 = Je + J\mathfrak{L} = Je + \mathfrak{L}$. Since $\mathfrak{L}$ is a left ideal, we must have $\mathfrak{L} = J\mathfrak{L}$. Since $\mathfrak{L}$ is nilpotent, the equation $\mathfrak{L} = J\mathfrak{L}$ implies $\mathfrak{L} = Je\mathfrak{L}$. From this last equation we obtain

$$e\mathfrak{L} + \mathfrak{C} = \mathfrak{L} = (eJe + \mathfrak{N}e)\mathfrak{L} = (eJe + \mathfrak{N}e)(e\mathfrak{L} + \mathfrak{C}) = e\mathfrak{L} + \mathfrak{N}e\mathfrak{L}.$$

Now the sum $e\mathfrak{L} + \mathfrak{C}$ is direct, and from the equations directly above we see that $\mathfrak{C}$ and $\mathfrak{N}e\mathfrak{L}$ are both complements of $e\mathfrak{L}$ in $\mathfrak{L}$. But $\mathfrak{N}e \cdot e\mathfrak{L}$ is obviously contained in both $\mathfrak{N}$ and $\mathfrak{L}$—i.e. $\mathfrak{N}e\mathfrak{L} \subseteq \mathfrak{C}$. Hence $\mathfrak{N}e\mathfrak{L} = \mathfrak{C}$.

This result may be stated as the following theorem:

6.8: *If $J$ is an idempotent* MLI *ring and $e$ is a principal idempotent of $J$, then in the decomposition $J = eJe + e\mathfrak{L} + \mathfrak{N}e + [\mathfrak{L}, \mathfrak{N}]$ we must have $[\mathfrak{L}, \mathfrak{N}] = \mathfrak{N}e\mathfrak{L}$.*

**7.** In this section we shall prove that an MLI ring of the most general type is the sum of an MLI idempotent ring and an MLI nilpotent ring.

Let $A$ be an MLI ring which is neither idempotent nor nilpotent. Now the rings $A, A^2, \cdots$ constitute a descending chain of left ideals of $A$:

$$A \supseteq A^2 \supseteq A^3 \supseteq \cdots. \tag{1}$$

Let $k$ be the smallest exponent for which $A^k = A^{k+1} = \cdots$. Then $A^k$, which we shall denote by $J$, is evidently both an idempotent ring and a two-sided ideal of $A$. Let $e$ be a principal idempotent of $A$, and consider the de-

composition

(2) $$A = eAe + e\mathfrak{L} + \mathfrak{R}e + \mathfrak{C}, \text{ where } \mathfrak{C} = [\mathfrak{L}, \mathfrak{R}].$$

Now $e$ is necessarily contained in $J$. So for $J$ we have the decomposition (3) $J = eJe + e\mathfrak{l} + \mathfrak{r}e + \mathfrak{c}$, where $\mathfrak{c} = [\mathfrak{l}, \mathfrak{r}]$ and $\mathfrak{l}(\mathfrak{r})$ is the left (right) annihilator of $e$ in $J$. Since $J$ is a two-sided ideal of $A$, it is easy to verify the following equations:

(4) $$eJe = eAe; \quad e\mathfrak{l} = e\mathfrak{L}; \quad \mathfrak{r}e = \mathfrak{R}e.$$

From 6.7 we know that $\mathfrak{c} = \mathfrak{r}e\mathfrak{l} = \mathfrak{R}e\mathfrak{L} \subseteq \mathfrak{C}$. Hence $[J, \mathfrak{C}] = \mathfrak{R}e\mathfrak{L}$. Now $\mathfrak{C}$ is a nilpotent MLI ring (see 4 ($\alpha$) & 4.2); and from 6.1 we know that $J$ is an MLI ring. So we have the following theorem.

7.1: *Any non-nilpotent* MLI *ring $A$ is the sum of a nilpotent* MLI *ring $B$ and an idempotent* MLI *ring $J$ which is a two-sided ideal of $A$. For the component $J$ we can always choose $A^k$, where $A^{k-1} \supset A^k = A^{k+1} = \cdots$; for the component $B$ we can select $[\mathfrak{L}, \mathfrak{R}]$, where $\mathfrak{L}$ and $\mathfrak{R}$ are respectively the left and right annihilators in $A$ of a principal idempotent of $A^k$. For these choices of $J$ and $B$ we have $[J, B] = \mathfrak{R}e\mathfrak{L}$.*

One can show by examples that it is not always possible to find a nilring $Q$ such that $A = A^k + Q$. If we choose $[\mathfrak{L}, \mathfrak{R}]$ as the component $B$ in $A = (A^k, B)$, it is an open question whether this $B$ is the same for all choices of $e$. Certainly $[\mathfrak{L}, \mathfrak{R}]$ depends on $A^k$ alone if $A^k$ contains a principal unit (two-sided identity element). And from 4.3 we obtain another case in which $[\mathfrak{L}, \mathfrak{R}]$ is independent of $e$.

7.2: *The component $[\mathfrak{L}, \mathfrak{R}]$ in the decomposition $A = (A^k, [\mathfrak{L}, \mathfrak{R}])$ is independent of $e$—i.e. depends on $A^k$ alone—whenever the exponent of the radical of $A$ does not exceed* 3.

**8.** Up to this point we have considered only MLI rings without operators. One naturally inquires, then, which of our results are valid for rings with operator domains. We shall attempt to answer the question in part for a ring $T$ having a domain of operators $\Omega$ such that each operator $\lambda$—which we shall write to the left of the elements of $T$—induces an endomorphism of $T$ which is an operator-endomorphism with respect to the elements of $T$ as both right-hand and left-hand operators. In symbols, we assume

(1) $$\lambda \cdot ab = \lambda a \cdot b = a \cdot \lambda b \text{ for } \lambda \in \Omega \quad \text{and} \quad a, b \in T.$$

First, let us consider the following question: if we are given a ring $A$ with minimal conditions for ordinary left ideals (MLI ring) and an operator domain $\Omega$ of the type above, which of the ideals $R$, $M_i$, $N_j$, etc. are admissible with respect to $\Omega$? We know, of course, that the homomorphic image of an ordinary left (right) ideal of $A$ with respect to an element $\lambda$ of $\Omega$ is an ordinary—but not necessarily an admissible—left (right) ideal of $A$. Now the radical $R$ of $A$

is the sum of all nilpotent left ideals u of $A$. Suppose that u is of exponent $\sigma$, and consider the product $\lambda u_1 \cdot \lambda u_2 \cdot \cdots \cdot \lambda u_{\sigma+1}$, where the $u$'s are $\sigma + 1$ arbitrary elements of u. By a repeated use of equations (1) we can bring this product to the form

$$u_1 \cdot u_2 \cdots u_\sigma \cdot u'_{\sigma+1}, \quad \text{where} \quad u'_{\sigma+1} = \lambda(\lambda(\cdots(\lambda u_{\sigma+1})\cdots)).$$

Hence $\lambda u$ is a nilpotent left ideal of exponent $\leqq \sigma + 1$, and is therefore contained in $R$. This proves that the radical of $A$ is an admissible left ideal.[27]

One can easily show that the annihilators $N_j$ and $M_j$ in §1 are all admissible ideals; this statement also holds for the components[28] $\mathfrak{L}$, $\mathfrak{R}$, $e\mathfrak{L}$, $\mathfrak{R}e$, $\mathfrak{C}$ in the various decompositions of $A$ with respect to a principal idempotent (see §§6–7). From the fact that $\lambda$ maps a minimal (nilpotent) left ideal onto a minimal (nilpotent) left ideal, it is easy to see that the sum of all minimal admissible left ideals (minimal nilpotent admissible left ideals) is the ideal $\mathfrak{M}$ (the ideal $\mathfrak{N}$) of §2.

Let us now consider the case of a ring $T$ with minimal condition for admissible left ideals (but not necessarily for ordinary left ideals). Such a ring we shall refer to as an AMLI ring. We assert that all the results in §§1–3 are valid if we replace the term "left ideal" by "admissible left ideal," "two-sided ideal" by "admissible left ideal and ordinary right ideal," "MLI ring" by "AMLI ring." One of the main results in §6 is undoubtedly Theorem 6.4, and this also holds for our ring $T$.

From the example in Footnote 27 one sees that for operator domains of a type more general than that of $\Omega$ we must either define the radical of our ring in terms of admissible nilpotent left ideals or else concede that the radical when defined in terms of ordinary nilpotent left ideals is not necessarily admissible. It is interesting to note that for the operator domain $\Omega$ these two methods of defining the radical lead to the same result.

TULANE UNIVERSITY,
NEW ORLEANS, LOUISIANA.

---

[27] This result is not trivial. The ring $J$ in Footnote 26 has a radical $R = Fu$. If $\varphi$ is the linear transformation defined by $\varphi e = u$ and $\varphi u = e$, it is easy to show that $\varphi \cdot ab = a \cdot \varphi b$ for all $a, b \in J$. One sees immediately that $R$ is not admissible with respect to $\varphi$, a situation which obviously arises from the fact that $\varphi \cdot ab$ is not always equal to $\varphi a \cdot b$.

[28] These components are admissible with respect to $\Omega$, in spite of the fact that they are not all left ideals of $A$. For instance, we have $\rho \cdot \lambda\mathfrak{R} = \lambda \cdot e\mathfrak{R} = 0$, which indicates that $\lambda\mathfrak{R}$ is contained in the right annihilator $\mathfrak{R}$ of $e$.